COMTREND CORPORATION

AR-5387un

ADSL2+ WLAN Router

Manual de Usuario

Versión C1.0, 24 de mayo de 2011

Prólogo

Este manual contiene información específica para la instalación y configuración de este dispositivo. Es de suponer que el lector de este manual posee conocimientos básicos de la terminología y los conceptos utilizados en telecomunicaciones.

Si descubre que el producto no funciona, o no lo hace de la forma adecuada, por favor, contacte con el servicio de soporte técnico para su inmediata reparación enviando un mensaje de correo electrónico a INT-support@comtrend.com

Para consultar cuestiones referentes a la actualización del producto, nuevos lanzamientos, revisión de manuales o actualizaciones de software, visite nuestro sitio Web en http://www.comtrend.com

Advertencias importante en materia de seguridad

Se recomienda seguir las siguientes recomendaciones básicas respecto al desembalaje, instalación, uso y mantenimiento de su dispositivo electrónico:

- Para evitar el riesgo de incendio o de descarga eléctrica no haga uso ni instale este dispositivo habiendo agua cerca. Por ejemplo cerca de una bañera, de un sumidero de cocina o lavadora, o cerca de una piscina. Tampoco exponga el equipo a la intemperie, lluvia o zonas húmedas (por ejemplo un suelo mojado).
- No conecte la fuente de alimentación en superficies a gran altura. Deje que el cable quede tendido. No debe haber obstáculos en su trayectoria, ni se deben colocar objetos pesados sobre el mismo. Además, no pise ni maltrate el cable de ninguna manera.
- Utilice únicamente el cable de alimentación y el adaptador que se adjunta con este dispositivo.
- Para salvaguardar el equipo del sobrecalentamiento, asegúrese de que ninguna de las aberturas de ventilación del equipo está obstruida.
- Evite el uso del teléfono (excepto los inalámbricos) durante una tormenta eléctrica. Existe un riesgo remoto de descarga eléctrica como consecuencia de los rayos. Así mismo, no utilice el teléfono para informar de una fuga de gas en las proximidades de la fuga.
- Nunca instale el cableado del teléfono durante condiciones atmosféricas de tormenta.

PRECAUCIÓN:

- Para evitar el riesgo de incendio utilice únicamente cable de comunicaciones del tipo AWG No. 26 o mayor.
- Desconecte siempre todos los cables telefónicos de los enchufes de pared antes de reparar o desmontar este equipo.

ADVERTENCIA

- Antes de abrir este equipo para su mantenimiento o revisión asegúrese de desconectar el cable de alimentación.
- En el Apéndice C - Especificaciones se recogen las especificaciones requeridas para el alimentador del dispositivo.

Copyright

Copyright© 2011 Comtrend Corporation. Todos los derechos reservados. La información y mensajes contenidos aquí son propiedad de Comtrend Corporation. Ninguna parte de este manual podrá ser traducida, transcrita, ni reproducida en forma alguna ni por ningún medio sin la previa autorización escrita de Comtrend Corporation.

Protección del medioambiente

Este símbolo indica que cuando el equipo haya alcanzado el final de su vida útil, deberá ser depositado en un centro de reciclaje y procesado de forma independiente de la basura doméstica.

La carcasa, el plástico contenido en el embalaje y las partes que conforman este router pueden reciclarse de acuerdo con las regulaciones locales. No se deshaga de este dispositivo electrónico en el mismo recipiente que la basura doméstica; ya que podría ser objeto de sanción o multas dispuestas por la ley. Por favor, sea responsable y obtenga información de su administración local sobre la forma idónea de deshacerse del equipo.

Índice de contenidos

CAPÍTULO 1 INTRODUCCIÓN 5
1.1 CARACTERÍSTICAS 5
1.2 USO 6

CAPÍTULO 2 INSTALACIÓN 7
2.1 INSTALACIÓN DEL HARDWARE 7
2.2 INDICADORES LED 9

CAPÍTULO 3 INTERFAZ WEB DE USUARIO 11
3.1 CONFIGURACIÓN PREDETERMINADA 11
3.2 CONFIGURACIÓN IP 11
3.3 PROCEDIMIENTO DE ACCESO 14

CAPÍTULO 4 INFORMACIÓN DEL DISPOSITIVO 16
4.1 WAN 17
4.2 ESTADÍSTICAS 18
4.2.1 Estadísticas LAN 18
4.2.2 Estadísticas WAN 19
4.2.3 Estadísticas xTM 20
4.2.4 Estadísticas xDSL 20
4.3 RUTAS 24
4.4 ARP 25
4.5 DHCP 26

CAPÍTULO 5 CONFIGURACIÓN AVANZADA 27
5.1 INTERFAZ LAYER 2 27
5.1.1 ATM Interface (Interfaz ATM) 27
5.2 SERVICIO WAN 28
5.3 LAN 29
5.4 NAT 31
5.4.1 Virtual Servers (Servidores virtuales) 31
5.4.2 Port Triggering (Redireccionamiento de puertos) 33
5.4.3 DMZ Host 34
5.5 SEGURIDAD 35
5.5.1 IP Filtering (Filtrado IP) 35
5.5.2 MAC Filtering (Filtrado MAC) 38
5.6 QOS (CALIDAD DE SERVICIO) 40
5.6.1 Queue Management Configuration (Configuración de gestión de la cola) 40
5.6.2 Queue Configuration (Configuración de la cola) 41
5.6.3 QoS Classification (Clasificación de QoS) 42
5.7 ROUTING 44
5.7.1 Default Gateway (Pasarela predeterminada) 44
5.7.2 Static Route (Ruta estática) 44
5.8 DNS 46
5.8.1 DNS Server (Servidor DNS) 46
5.8.2 Dynamic DNS (DNS Dinámico) 46
5.9 DSL 48
5.10 UPNP 51
5.11 PROXY DNS 52
5.12 SERVIDOR DE IMPRESIÓN 53
5.13 SERVICIO DE ALMACENAMIENTO 53
5.13.1 Storage Device Info (Información de Dispositivos de Almacenamiento) 54
5.13.2 FTP Configuration (Configuración FTP) 54
5.13.3 Samba Configuration (Configuración Samba) 55
5.14 INTERFACE GROUPING 56

CAPÍTULO 6 FUNCIÓN INALÁMBRICA 58
6.1 BASIC (BÁSICO) 58
6.2 SECURITY (SEGURIDAD) 60

6.2.1 WPS *62*
6.3 MAC FILTER (FILTRO MAC) 67
6.4 WIRELESS BRIDGE (PUENTE INALÁMBRICO) 68
6.5 ADVANCED (FUNCIÓN INALÁMBRICA AVANZADA) 69
6.6 STATION INFO (INFORMACIÓN DE LA ESTACIÓN) 73

CAPÍTULO 7 DIAGNÓSTICOS 74

CAPÍTULO 8 ADMINISTRACIÓN 75
8.1 SETTINGS (CONFIGURACIÓN) 75
8.1.1 Backup Settings (Copia de seguridad de la Configuración) *75*
8.1.2 Update Settings (Restablecimiento de la configuración guardada) *75*
8.1.3 Restore Default (Restablecimiento de la configuración predeterminada) *76*
8.2 SYSTEM LOG (REGISTRO DEL SISTEMA) 77
8.3 SECURITY LOG (REGISTRO DE SEGURIDAD) 79
8.4 INTERNET TIME (HORA DE INTERNET) 80
8.5 ACCESS CONTROL (CONTROL DE ACCESO) 81
8.5.1 Password (Contraseñas) *81*
8.6 UPDATE SOFTWARE (ACTUALIZACIÓN) 82
8.7 REBOOT (REINICIAR) 83

APÉNDICE A – FIREWALL (CORTAFUEGOS) 84

APÉNDICE B - ASIGNACIÓN DE PINS 87

APÉNDICE C - ESPECIFICACIONES 89

APÉNDICE D – CLIENTE SSH 91

APÉNDICE E – FUNCIONAMIENTO WPS 92

APÉNDICE F – SERVIDOR DE IMPRESIÓN 95

APÉNDICE G – INSTALACIÓN DE LA CONEXIÓN 101

Capítulo 1 Introducción

El AR-5387un es un router ADSL inalámbrico de alto rendimiento, que alcanza una velocidad máxima de 1 Mbps en el sentido de subida de datos y 24 Mbps en el sentido de bajada.

El AR-5387un incluye cuatro puertos 10/100 Base-T Ethernet, un interfaz de línea RJ11 y un Host USB 2.0, que puede soportar un servidor de impresión. Constituye la solución de banda ancha ideal tanto para usuarios domésticos que desean compartir acceso a Internet de alta velocidad como para pequeñas oficinas que operan en Internet.

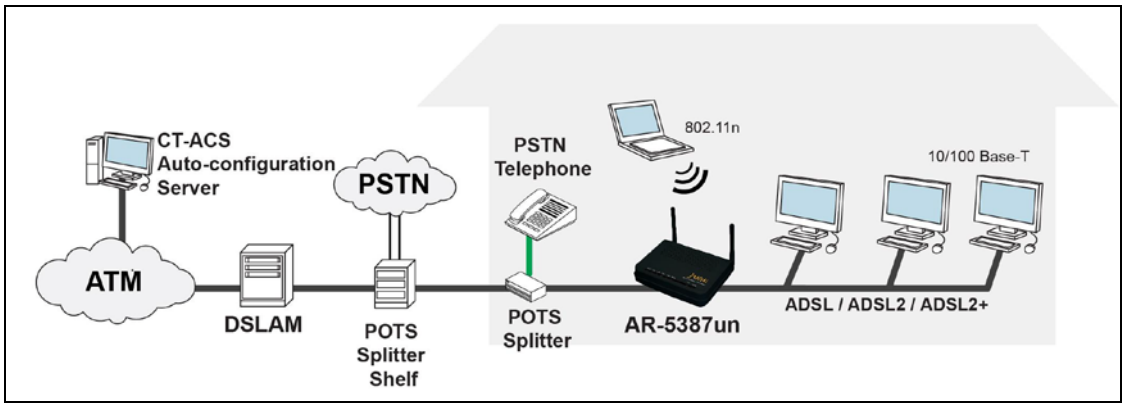
El router AR-5387un incorpora un interfaz gráfico de usuario basado en web (GUI), a través del cual es sencillo modificar la configuración del router o conectarse al ISP correspondiente. También proporciona estadísticos de tráfico, indicadores del estado de la conexión y otra información detallada. El router AR-5387un soporta direccionamiento IP estático o dinámico y conectividad PPPoE.

1.1 Características

- Punto de Acceso integrado 802.11n (compatible con 802.11b/g)
- AR-5387un (Anexo A)
- Calidad de servicio (QoS) tanto IP como de circuito virtual (VC) a nivel de paquete
- Sistema inalámbrico 2x2 MIMO
- WPA/WPA2 y 802.1x
- WPS (Wi-Fi Protected Setup)
- Sistema de Distribución Inalámbrico (WDS)
- Direccionamiento estático RIP/RIP v2
- Soporte para PPPoE/PPPoA/IPoA/MER
- Gestión basada en interfaz Web
- Soporta administración remota
- Restauración y copia de seguridad de la configuración
- Actualización de firmware y configuración
- Soporta TR-069/TR-098/TR-111 para gestión remota
- NAT/PAT
- Proxy IGMP
- Configuración Auto PVC
- Soporta hasta 8 CVs
- WMM y UPnP
- Filtrado de direcciones IP/MAC
- Múltiples SSID
- Servidor/Relay/Cliente DHCP
- Proxy DNS
- Servidor FTP/TFTP

1.2 Uso

El siguiente diagrama describe la utilización típica del AR-5387un.

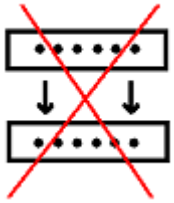


Capítulo 2 Instalación

2.1 Instalación del hardware

Siga las siguientes instrucciones para completar la instalación del hardware.

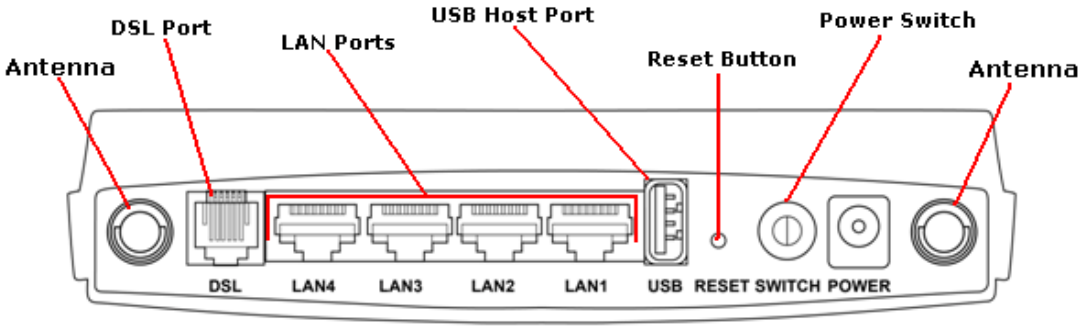
No apilable



Este dispositivo no es apilable. No colocar unidades una encima de otra. De lo contrario, podrían resultar dañadas.

PANEL POSTERIOR

La siguiente imagen muestra el panel posterior del dispositivo.



DSL
Conecte el cable DSL RJ11 al puerto DSL.

Puertos LAN (Ethernet)
Puede conectar hasta cuatro dispositivos LAN al router usando cables RJ45. Estos puertos son auto-sensing MDI/X; con lo que puede utilizar cable plano (straight-through) o cruzado (crossover).

Puerto Host USB (Tipo A)
Este puerto puede usarse para conectar una impresora o dispositivos de almacenamiento masivo.

Botón Reset
Para restaurar la configuración de fábrica del dispositivo mantenga pulsado el botón Reset de 5 a 10 segundos. Una vez que el dispositivo se haya reiniciado correctamente el panel frontal mostrará la disposición de indicadores luminosos esperada (véase la sección 2.2 Indicadores LED para más detalles).

NOTA: Si se mantiene pulsado el botón Reset durante más de 20 segundos, el router AR-5387un entrará en modo de actualización de firmware (modo de inicio CFE). El firmware puede entonces ser actualizado a través del navegador de Internet que apunte a la dirección IP predeterminada.

Encendido

Presione el botón de encendido a la posición de OFF (botón fuera). Conecte la fuente de alimentación en la clavija hembra de alimentación del dispositivo. Conecte la fuente de alimentación a un enchufe de la pared u otra fuente de corriente alterna. Presione el botón de encendido a la posición de ON (botón dentro). Si el LED se enciende como era de esperar, el dispositivo estará listo para su configuración (véase sección 2.2 Indicadores LED).

PRECAUCIÓN 1: Si el router falla en el encendido, o no funciona correctamente, primero compruebe que el cable de alimentación está correctamente conectado. Encienda entonces el router nuevamente. Si el problema persiste, contacte con nuestro soporte técnico.

PRECAUCIÓN 2: Antes de realizar cualquier tarea de mantenimiento de este equipo, desconecte siempre el cable de alimentación y de teléfono de las tomas de la pared.

2.2 Indicadores LED

Los indicadores luminosos LED del panel frontal se muestran a continuación y se describen en la siguiente tabla.
Esta información puede utilizarse para comprobar el estado del dispositivo y sus conexiones.

LED	Color	Modo	Función
POWER	Verde	Encendido	El dispositivo está encendido.
		Apagado	El dispositivo está apagado.
	Rojo	Encendido	POST (Power On Self Test) fallo u otro malfuncionamiento. Un malfuncionamiento es cualquier error de la secuencia interna o estado que imposibilita la conexión a la DSLAM o el paso de datos del cliente.
LAN 1X-4X	Verde	Encendido	Se ha establecido una conexión Ethernet.
		Apagado	No se ha establecido una conexión Ethernet.
		Intermitente	Transmitiendo o recibiendo datos por la LAN.
WLAN	Verde	Encendido	El módulo inalámbrico está listo. (instalado y activado).
		Apagado	El módulo inalámbrico no está listo. (no instalado o desactivado)
		Intermitente	Transmitiendo o recibiendo datos por la WLAN.
DSL	Verde	Encendido	Se ha establecido una conexión xDSL.
		Apagado	No se ha establecido una conexión xDSL
		Intermitente	rápido: la conexión xDSL está sincronizando o transmitiendo datos. despacio: El sincronismo xDSL ha fallado.
INTERNET	Verde	Encendido	Conexión IP activa y sin tráfico. Si la sesión IP o PPPoE se termina debido a la finalización del tiempo límite de inactividad, el LED permanecerá encendido en verde siempre y cuando la conexión ADSL permanezca establecida.
		Apagado	Modem apagado o en modo bridge, o conexión ADSL no establecida. Si una sesión IP o PPPoE se termina por cualquier causa distinta del tiempo límite de inactividad, el LED se apagará.

		Intermitente	Conexión IP activa y con tráfico en proceso (en cualquiera de los dos sentidos, ascendente o descendente)

Capítulo 3 Interfaz Web de Usuario

Esta sección describe la forma de acceder al dispositivo mediante una interfaz Web de usuario (WUI) a través de un navegador como Internet Explorer (versión 5.0 y posteriores).

3.1 Configuración predeterminada

La configuración predeterminada de fábrica de este dispositivo se resume a continuación.

- Dirección IP LAN: 192.168.1.1
- Máscara de subred LAN: 255.255.255.0
- Acceso de administración (nombre de usuario: **admin**, contraseña: **admin**)
- Acceso de usuario (nombre de usuario: **user**, contraseña: **user**)
- Acceso a la WLAN: **activado**

Nota Técnica

Cuando se enciende, el dispositivo se pone en marcha con todos sus valores predeterminados. Entonces lee el perfil de configuración desde la sección de almacenamiento permanente de la memoria flash. Los valores de los parámetros predeterminados son sobrescritos cuando se configuran idénticos parámetros con valores distintos. El perfil de configuración del área de almacenamiento permanente puede crearse a través de la interfaz de Web de usuario, mediante una interfaz telnet o mediante cualquier otro protocolo de gestión. La configuración de fábrica puede ser restaurada o bien pulsando el botón Reset durante más de 5 segundos hasta que el LED de encendido parpadee o bien haciendo clic en la opción Default Configuration en la pantalla Restore Settings.

3.2 Configuración IP

MODO DHCP

Cuando se enciende el AR-5387un se activa el servidor DHCP integrado. Básicamente lo que hace el servidor DHCP es gestionar y reservar las direcciones IP para los dispositivos LAN como, por ejemplo, su PC.

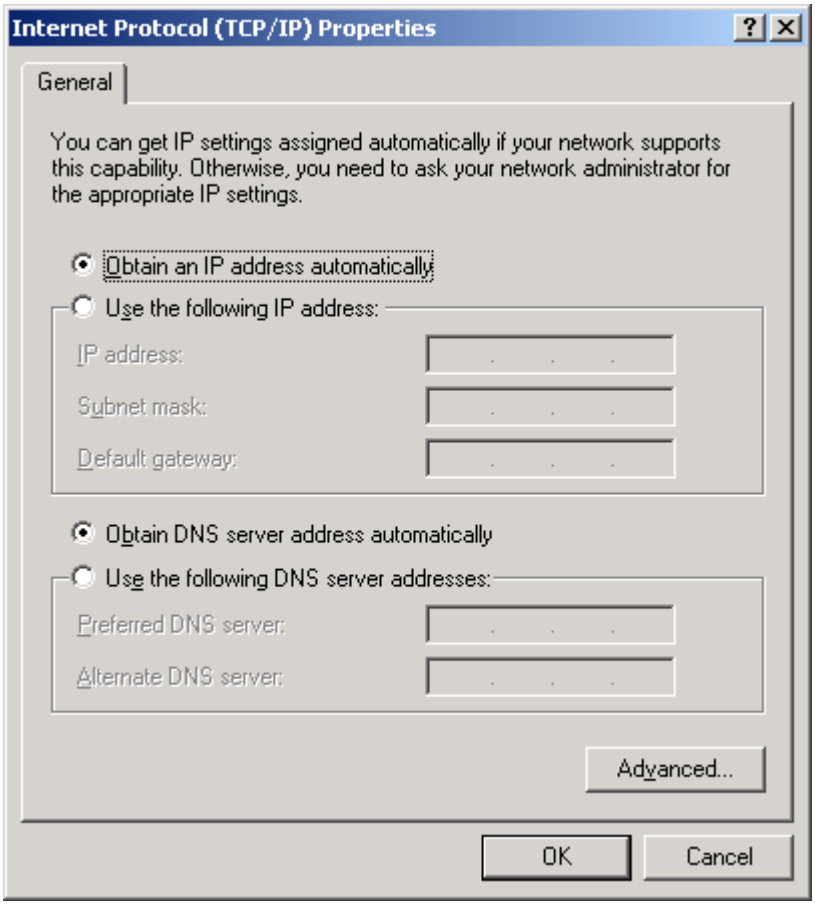
Para obtener una dirección IP desde el servidor DHCP siga los siguientes pasos.

NOTA:	El siguiente procedimiento asume que está ejecutando Windows XP. Sin embargo, los pasos generales involucrados son similares en la mayoría de los sistemas operativos (SO). Compruebe la documentación de soporte de su sistema operativo para conocer más detalles.

PASO 1: Desde la ventana de Conexiones de red, abra Conexión de área local (*también puede acceder a esta ventana haciendo doble clic en el icono Conexión de área local es su barra de tareas*). Haga clic sobre el botón **Propiedades**.

PASO 2: Seleccione Protocolo Internet (TCP/IP) y haga clic en el botón de Propiedades.

PASO 3: Seleccione obtener una dirección IP automáticamente como se muestra más abajo.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

PASO 4: Haga clic sobre **Aceptar** para aplicar los cambios.

Si le surge alguna dificultad con el modo DHCP puede probar a establecer una IP estática en su lugar.

MODO IP ESTÁTICA

En el modo de IP estática, puede aplicar la configuración de IP para su PC de forma manual.

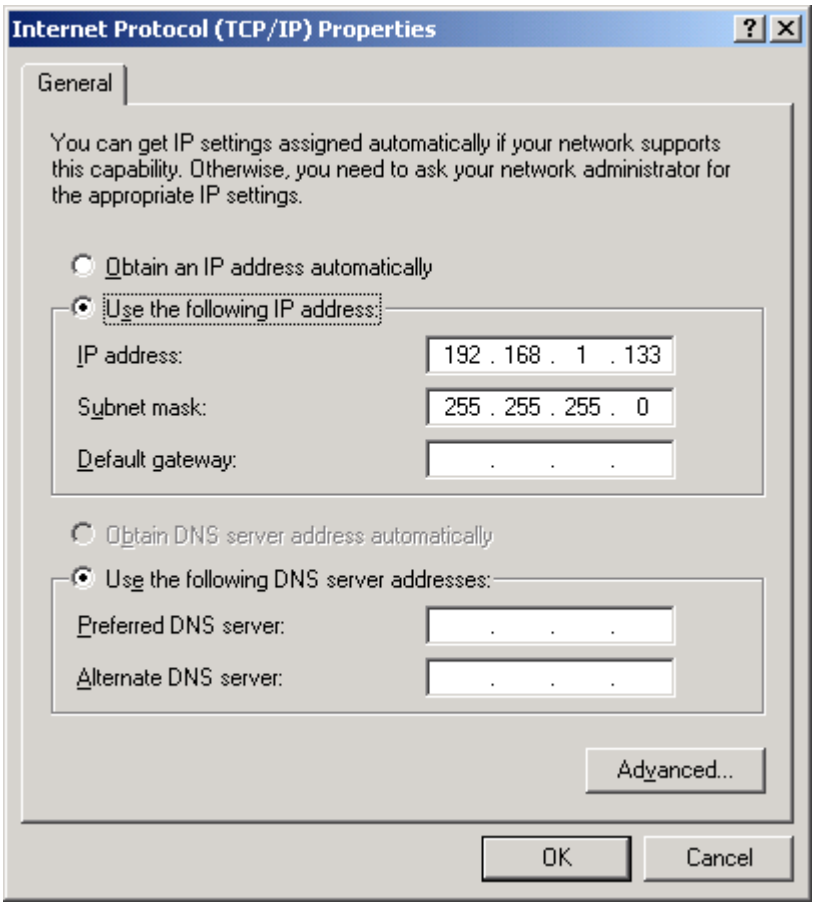
Siga los siguientes pasos para configurar la dirección IP de su PC para que utilice la subred 192.168.1.x.

NOTA:	El siguiente procedimiento asume que está ejecutando Windows XP. Sin embargo, los pasos generales involucrados son similares en la mayoría de los sistemas operativos (SO). Compruebe la documentación de soporte de su sistema operativo para conocer más detalles.

PASO 1: Desde la ventana Conexiones de red, abra Conexión de área local (también puede acceder a esta ventana haciendo doble clic en el icono Conexión de área local en su barra de tareas). Haga clic sobre el botón **Propiedades**.

PASO 2: Seleccione Protocolo Internet (TCP/IP) y haga clic sobre el botón Propiedades.

Paso 3: Cambie la dirección IP a la subred 192.168.1.x (1<x<255) con la máscara de subred 255.255.255.0. La pantalla debería aparecer como se muestra a continuación.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 133
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

PASO 4: Haga clic sobre **Aceptar** para aplicar los cambios.

3.3 Procedimiento de acceso

Ejecute los siguientes pasos para abrir la interfaz Web de usuario.

NOTA:	Los ajustes predeterminados puede encontrarlos en la sección 3.1 Configuración predeterminada

PASO 1: Inicie su navegador de Internet. Escriba la dirección IP del dispositivo en el campo Dirección del navegador. Por ejemplo, si la dirección IP es 192.168.1.1, escriba http://192.168.1.1.

NOTA:	Para la gestión local (es decir, el acceso LAN), el PC que ejecute el navegador deberá estar conectado a Ethernet y no necesariamente al dispositivo. Para el acceso remoto (por ejemplo WAN), use la dirección IP mostrada en la pantalla del Capítulo 4 Información del dispositivo y acceda con el nombre de usuario y contraseña adecuados.

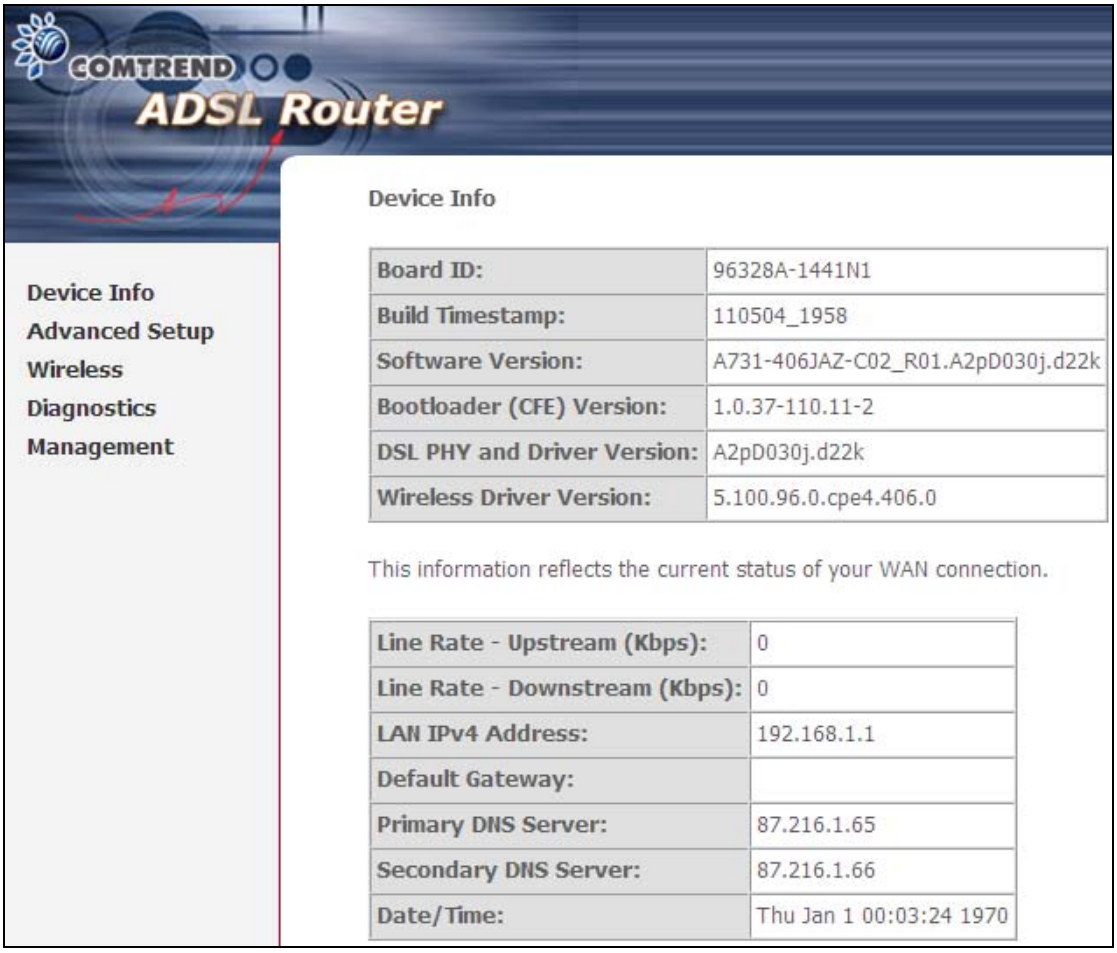
PASO 2: Se mostrará un cuadro de diálogo como el que puede verse debajo. Introduzca el nombre de usuario y la contraseña como se definieron en la sección 3.1 Configuración predeterminada.

Connect to 192.168.1.1
The server 192.168.1.1 at Broadband Router requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

Haga clic sobre **OK** para continuar.

NOTA:	La contraseña de acceso puede cambiarse más tarde. Véase la sección 8.5.1 Password (Contraseñas).

PASO 3: Tras acceder por primera vez se mostrará esta pantalla:



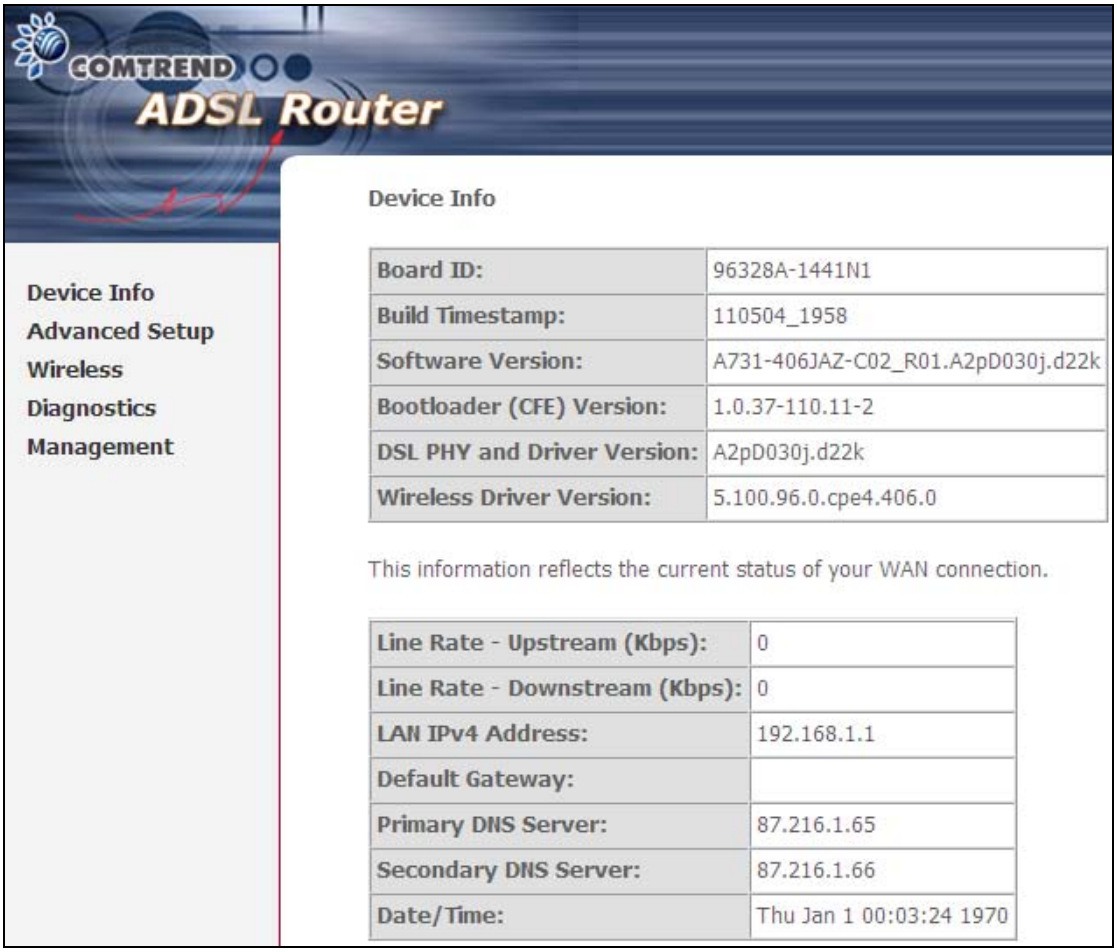
Capítulo 4 Información del dispositivo

La ventana de la interfaz Web de usuario está dividida en dos partes, el menú principal en el lado izquierdo y la pantalla de visualización a la derecha. El menú principal tiene varias opciones y seleccionando cada una de estas opciones se abre un submenú con más opciones de selección.

NOTA:	Los elementos del menú que se muestran varían en función de las conexiones configuradas y de los privilegios de la cuenta del usuario. Por ejemplo, si NAT y Firewall están activos, el menú principal mostrará los submenús NAT y Security. Si, por el contrario, están desactivados, sus correspondientes menús también lo estarán.

Device Info (Información del dispositivo) es la primera opción de selección en el menú principal, por lo que se comentará en primer lugar. En los siguiente capítulos se presentarán el resto de opciones del menú principal de forma correlativa.

La pantalla Device Info Summary (Resumen de información del dispositivo) aparece al inicio.



Esta pantalla muestra las configuraciones de hardware, software e IP, además de otra información relacionada.

4.1 WAN

Seleccione WAN desde el submenú de Device Info para ver los Pécs configurados.

Encabezado	Descripción
Interface	Nombre de la interfaz para WAN
Description	Nombre de la conexión WAN
Type	Muestra el tipo de conexión
VlanMuxId	Muestra el ID 802.1Q VLAN
IGMP	Muestra el estado del Protocolo de Gestión de Grupo de Internet (IGMP)
NAT	Muestra el estado del Network Address Translation (NAT)
Firewall	Muestra el estado del Firewall (Cortafuegos)
Status	Muestra el estado de la conexión DSL
IPv4 Address	Muestra la dirección WAN IPv4

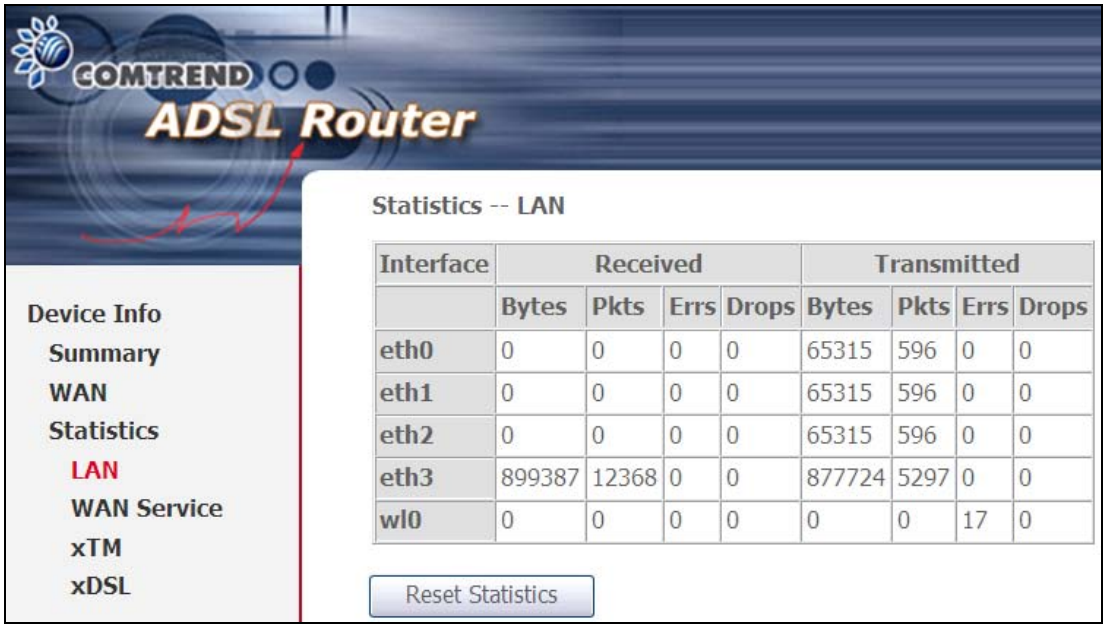
4.2 Estadísticas

Esta sección proporciona datos estadísticos sobre la interfaz de red LAN, WAN, ATM/PTM y xDSL.

NOTA:	Estas pantallas se actualizan cada 15 segundos de forma automática. Haga clic sobre **Reset Statistics** para provocar una actualización manual.

4.2.1 Estadísticas LAN

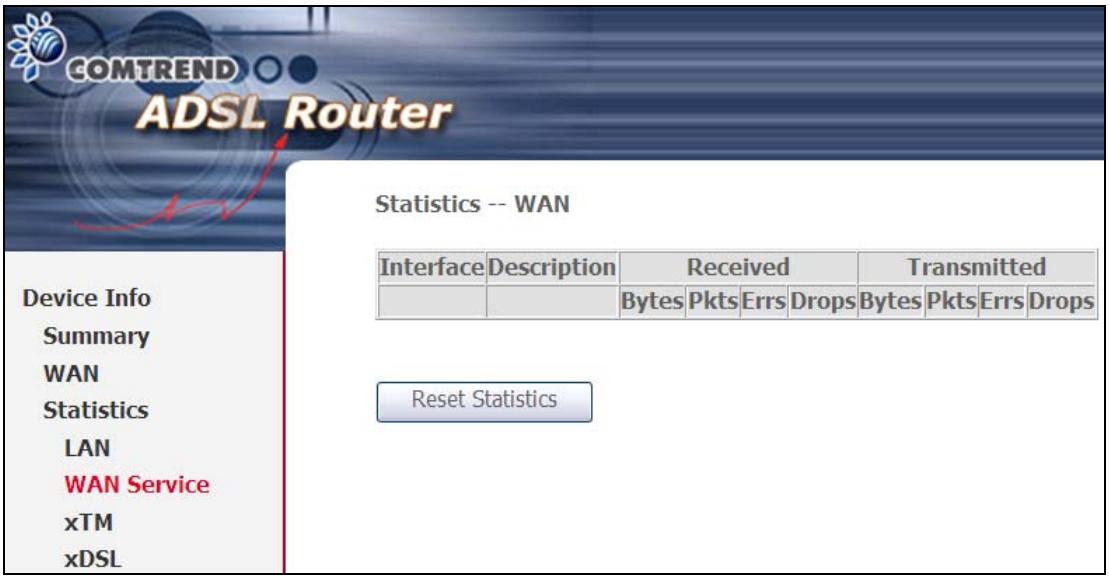
Esta pantalla muestra las estadísticas sobre la transmisión de datos de cada interfaz LAN.



Encabezado		Descripción
Interface		Interfaces LAN
Received/Transmitted:	- Bytes - Pkts - Errs - Drops	Número de Bytes Número de Packets Número de Packets con error Número de Packets rechazados

4.2.2 Estadísticas WAN

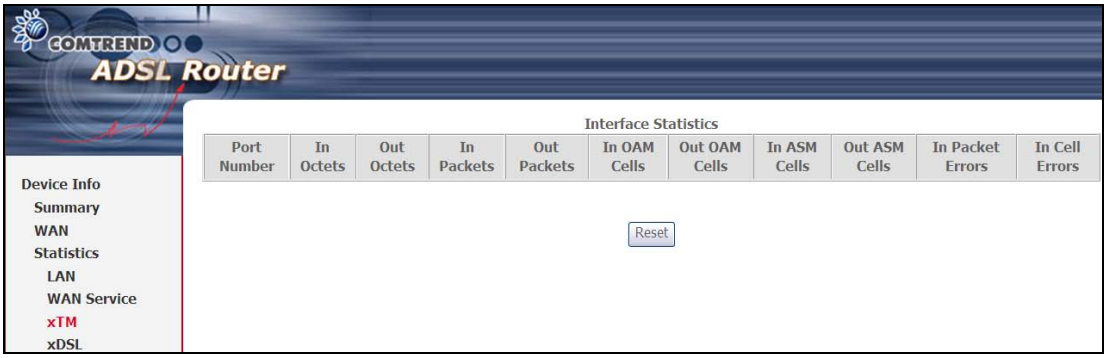
Esta pantalla muestra las estadísticas sobre la transmisión de datos de cada interfaz WAN.



Encabezado	Descripción
Interface	Interfaces WAN
Description	Etiqueta de servicio WAN
Received/Transmitted: - Bytes - Pkts - Errs - Drops	Número de Bytes Número de Packets Número de Packets con error Número de Packets rechazados

4.2.3 Estadísticas xTM

La siguiente imagen muestra estadísticas del Modo de Transferencia Asincrona (xTM).



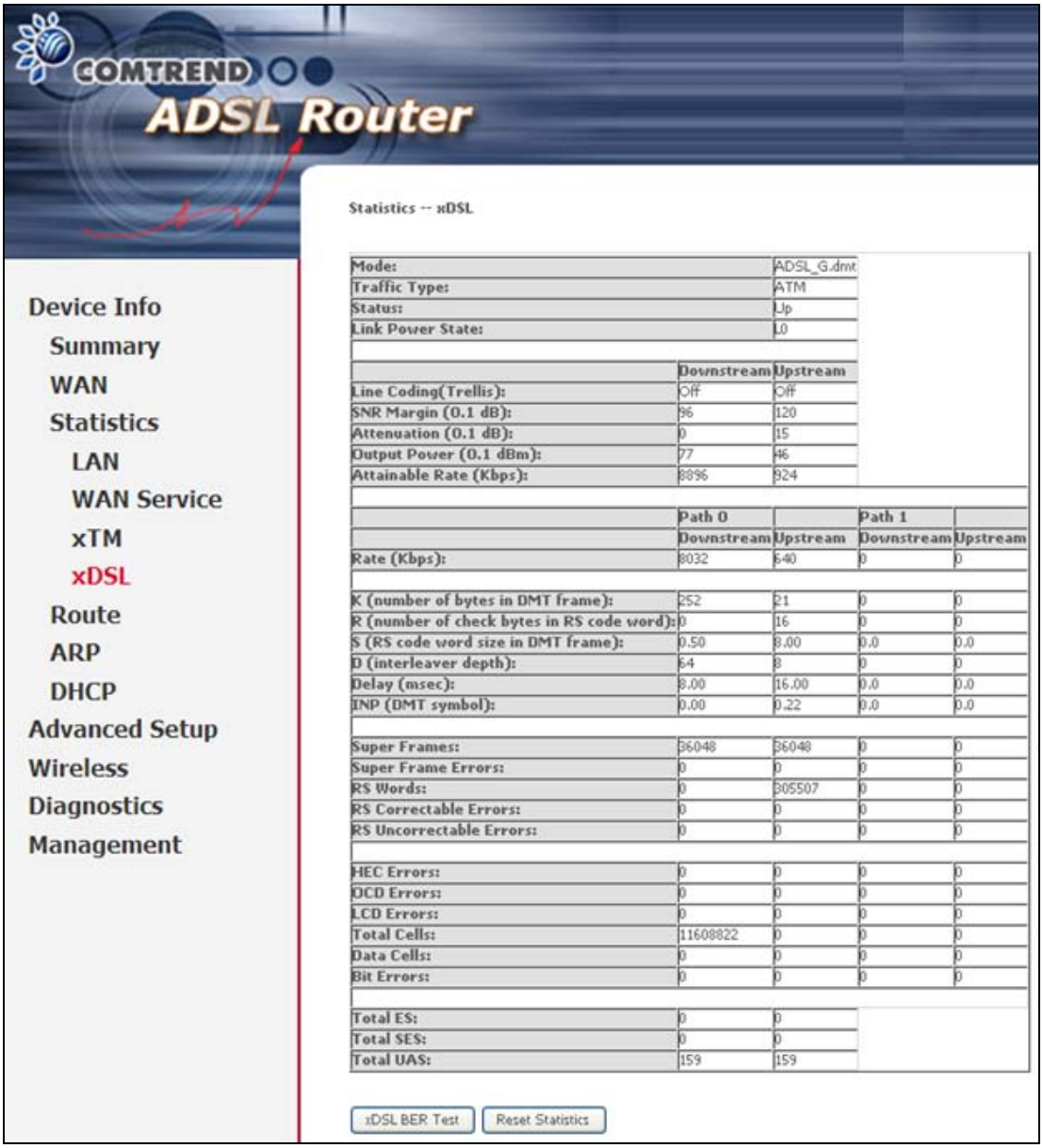
Estadísticas del interfaz ATM

Encabezado	Descripción
Port Number	PUERTO ATM (0-3)
In Octets	Número de octetos recibidos a través de la interfaz
Out Octets	Número de octetos transmitidos a través de la interfaz
In Packets	Número de paquetes recibidos a través de la interfaz
Out Packets	Número de paquetes transmitidos a través de la interfaz
In OAM Cells	Número de celdas OAM recibidas a través del interfaz
Out OAM Cells	Número de celdas OAM transmitidas a través del interfaz
In ASM Cells	Número de celdas ASM recibidas a través del interfaz
Out ASM Cells	Número de celdas ASM transmitidas a través del interfaz
In Packet Errors	Número de paquetes erróneos recibidos
In Cell Errors	Número de celdas erróneas recibidas

4.2.4 Estadísticas xDSL

La pantalla xDSL Statistics muestra información correspondiente al tipo de xDSL.

ADSL


COMTREND
ADSL Router
Device Info
Summary
WAN
Statistics
LAN
WAN Service
xTM
xDSL
Route
ARP
DHCP
Advanced Setup
Wireless
Diagnostics
Management
Statistics -- xDSL
Mode: ADSL_G.dmt
Traffic Type: ATM
Status: Up
Link Power State: L0
Downstream Upstream
Line Coding(Trellis): Off Off
SNR Margin (0.1 dB): 96 120
Attenuation (0.1 dB): 0 15
Output Power (0.1 dBm): 77 46
Attainable Rate (Kbps): 8896 924
Path 0 Path 1
Downstream Upstream Downstream Upstream
Rate (Kbps): 8032 640 0 0
K (number of bytes in DMT frame): 252 21 0 0
R (number of check bytes in RS code word): 0 16 0 0
S (RS code word size in DMT frame): 0.50 8.00 0.0 0.0
D (interleaver depth): 64 8 0 0
Delay (msec): 8.00 16.00 0.0 0.0
INP (DMT symbol): 0.00 0.22 0.0 0.0
Super Frames: 36048 36048 0 0
Super Frame Errors: 0 0 0 0
RS Words: 0 305507 0 0
RS Correctable Errors: 0 0 0 0
RS Uncorrectable Errors: 0 0 0 0
HEC Errors: 0 0 0 0
OCD Errors: 0 0 0 0
LCD Errors: 0 0 0 0
Total Cells: 11608822 0 0 0
Data Cells: 0 0 0 0
Bit Errors: 0 0 0 0
Total ES: 0 0
Total SES: 0 0
Total UAS: 159 159
xDSL BER Test
Reset Statistics

Haga clic en el botón **Reset Statistic** para actualizar esta pantalla.

Campo	Descripción
Mode	Protocolo de modulación G.Dmt, G.lite, T1.413, ADSL2, ADSL2+
Traffic Type	Intercalado del tipo de canal o Fast
Status	Muestra el estado de la conexión DSL
Link Power State	Estado de la potencia de salida de la conexión
Line Coding (Trellis)	Trellis Encendido/Apagado
SNR Margin (0.1 dB)	Margen de relación señal/ruido (SNR)
Attenuation (0.1 dB)	Atenuación media estimada del bucle en bajada
Output Power (0.1 dBm)	Corriente de salida de subida total

Campo	Descripción
Attainable Rate (Kbps)	Tasa de sincronismo obtenida
Rate (Kbps)	Tasa actual de sincronismo de bajada/subida

En el modo ADSL2+ se añade la siguiente sección.

MSGc	Número de bytes en el mensaje de canal de cabecera
B	Número de bytes en la Trama de datos de Mux
M	Número de Tramas de datos de Mux en la Trama de Datos FEC
T	Tramas de datos de Mux sobre bytes de sincronismo
R	Número de bytes de comprobación en la Trama de datos de FEC
S	Ratio de FEC sobre longitud de Trama de Datos PMD
L	Número de bytes en la Trama de datos PMD
D	Profundidad del intercalador
Delay	El retardo en milisegundos (msec)
INP	DMT symbol

En el modo G.DMT se añade la siguiente sección.

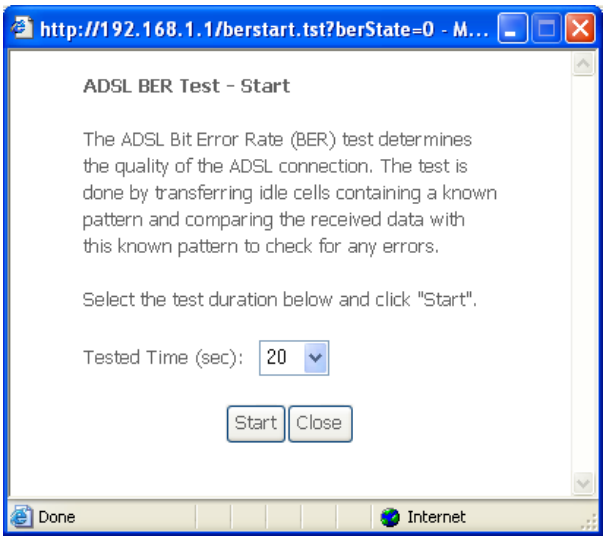
K	Número de bytes en Trama DMT
R	Número de bytes de comprobación por palabra de código RS
S	Tamaño por palabra de código RS en trama DMT
D	Profundidad del intercalador
Delay	El retardo en milisegundos (msec)

OH Frames	Número total de tramas OH
OH Frame Errors	Número de tramas OH recibidas con error
RS Words	Número total de errores de código Reed-Solomon
RS Correctable Errors	Número total de RS con errores recuperables
RS Uncorrectable Errors	Número total de RS con errores irrecuperables

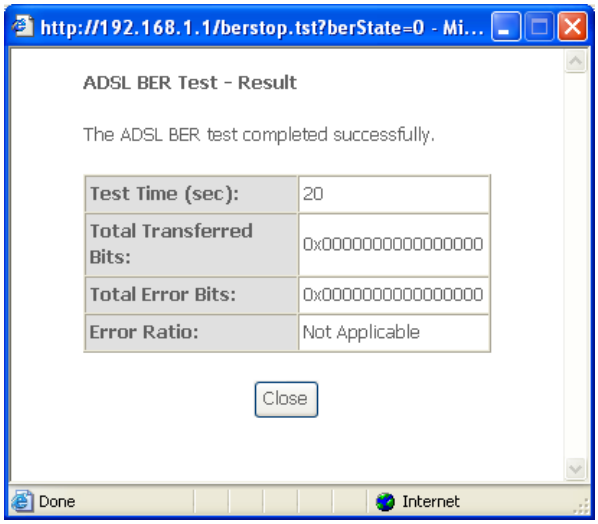
HEC Errors	Número total de errores Header Error Checksum
OCD Errors	Número total de errores de delineación fuera de celda (OCD Errors)
LCD Errors	Número total de errores de delineación de pérdida de celdas (LCD Errors)
Total Cells	Número total de celdas ATM (incluidas celdas inactivas y de datos)
Data Cells	Número total de celdas de datos ATM
Bit Errors	Número total de errores de bit
Total ES	Número total de segundos de error
Total SES	Número total de segundos de error graves
Total UAS	Número total de segundos de no disponibilidad

TEST xDSL BER

Haga clic sobre **xDSL BER Test** en la pantalla xDSL Statistics para comprobar el Bit Error Rate (BER) Una vez pulsado el botón se abrirá una pequeña ventana emergente como la que se muestra debajo.

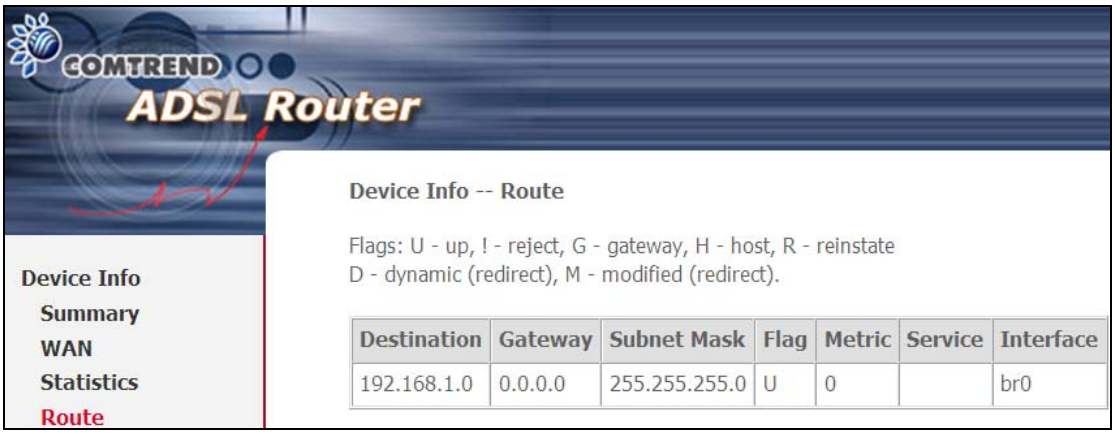

http://192.168.1.1/berstart.tst?berState=0 - M...
ADSL BER Test - Start
The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.
Select the test duration below and click "Start".
Tested Time (sec): 20
Start
Close
Done
Internet

Haga clic en **Start** para iniciar el test o en **Close** para cancelarlo. Una vez que se haya completado el test BER, aparecerá la siguiente ventana emergente.



4.3 Rutas

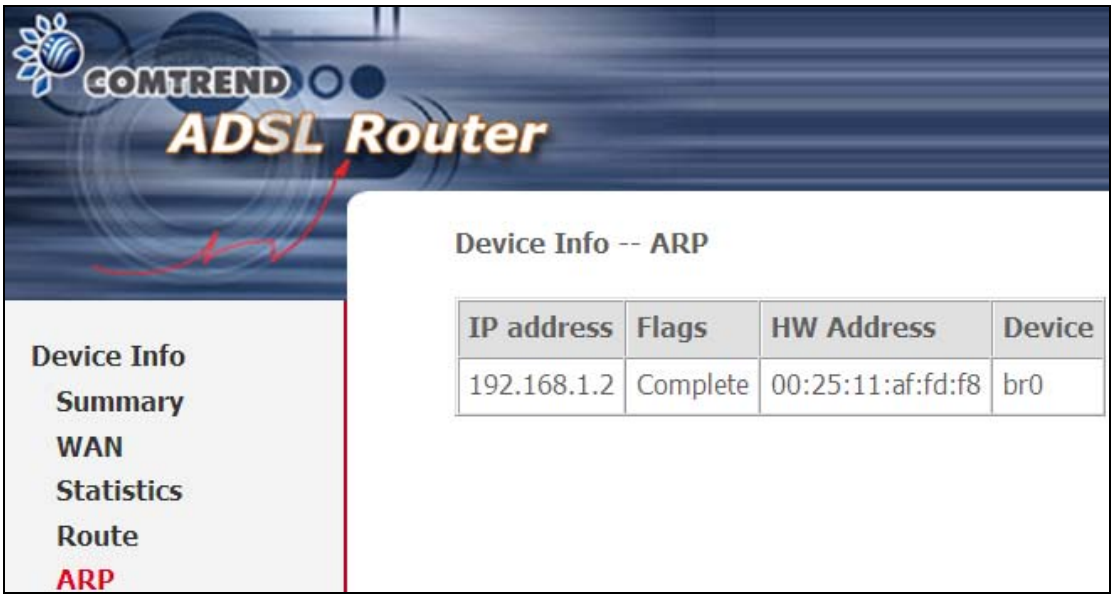
Escoja **Route** para ver las rutas que el AR-5387un ha encontrado.


COMTREND
ADSL Router
Device Info -- Route
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).
Device Info
Summary
WAN
Statistics
Route
Destination Gateway Subnet Mask Flag Metric Service Interface
192.168.1.0 0.0.0.0 255.255.255.0 U 0 br0

Campo	Descripción
Destination	Red o host de destino
Gateway	Próxima dirección IP de la puerta de enlace (hub)
Subnet Mask	Máscara de subred de destino
Flag	U: ruta está activada !: rechaza ruta G: usa pasarela H: destino es un host R: restablece la ruta para enrutamiento dinámico D: instalado dinámicamente por daemon o redireccionar M: modificado desde el enrutamiento daemon o redireccionar
Metric	La “distancia” al destino, normalmente contabilizada en saltos, no es utilizada por los kernels más recientes, pero puede ser necesaria para los daemons de enrutamiento.
Service	Muestra la etiqueta de conexión WAN
Interface	Muestra los interfaces de conexión

4.4 ARP

Haga clic sobre **ARP** para ver la información ARP.



Campo	Descripción
IP address	Muestra la dirección IP del PC host
Flags	Completo, Incompleto, Permanente o Público
HW Address	Muestra la dirección MAC del PC host
Device	Muestra la interfaz de conexión

4.5 DHCP

Haga clic sobre **DHCP** para ver la información sobre asignaciónes DHCP.

Campo	Descripción
Hostname	Muestra el nombre de red del dispositivo/host/PC
MAC Address	Muestra la dirección MAC Ethernet del dispositivo/host/PC
IP Address	Muestra la dirección IP del dispositivo/host/PC
Expires In	Muestra cuanto tiempo queda para que caduque cada asignación DHCP

Capítulo 5 Configuración avanzada

5.1 Interfaz Layer 2

Se describe aquí la pantalla del interfaz ATM

5.1.1 ATM Interface (Interfaz ATM)

Aquí puede añadir o eliminar conexiones de interfaz ATM.

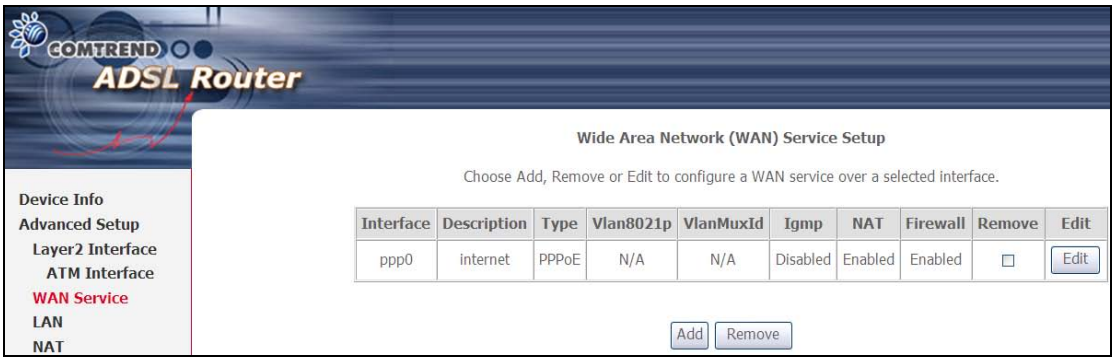
Haga clic sobre **Add** para crear una nueva interfaz ATM (véase Apéndice G – Instalación de la conexión).

NOTA:	Pueden crearse hasta 8 interfaces ATM y guardarse en la memoria Flash.

Para eliminar una conexión marque la casilla ☑ de la columna Remove y haga clic en **Remove**.

5.2 Servicio WAN

Esta pantalla permite la configuración de interfaces WAN.



Haga clic sobre el botón **Add** para crear una nueva conexión. Para las conexiones con interfaces ATM o WAN ETH véase Apéndice G – Instalación de la conexión.

NOTA:	No pueden coexistir conexiones de servicio ETH y ATM. En el modo predeterminado pueden configurarse hasta 8 conexiones WAN; los modos de conexión VLAN Mux y MSC soportan hasta 8 conexiones WAN.

Para eliminar una conexión marque la casilla ☑ de la columna Remove y haga clic en **Remove**.

Encabezado	Descripción
Interface	Nombre de la interfaz para WAN
Description	Nombre de la conexión WAN
Type	Muestra el tipo de conexión
Vlan8021p	VLAN ID es utilizado para el etiquetado VLAN (IEEE 802.1Q)
VlanMuxId	Muestra el ID 802.1Q VLAN
IGMP	Muestra el estado del Protocolo de Gestión de Grupo de Internet (IGMP)
NAT	Muestra el estado del Network Address Translation (NAT)
Firewall	Muestra el estado de seguridad
Remove	Selecciona la interfaz a eliminar
Edit	Selecciona la interfaz para editar

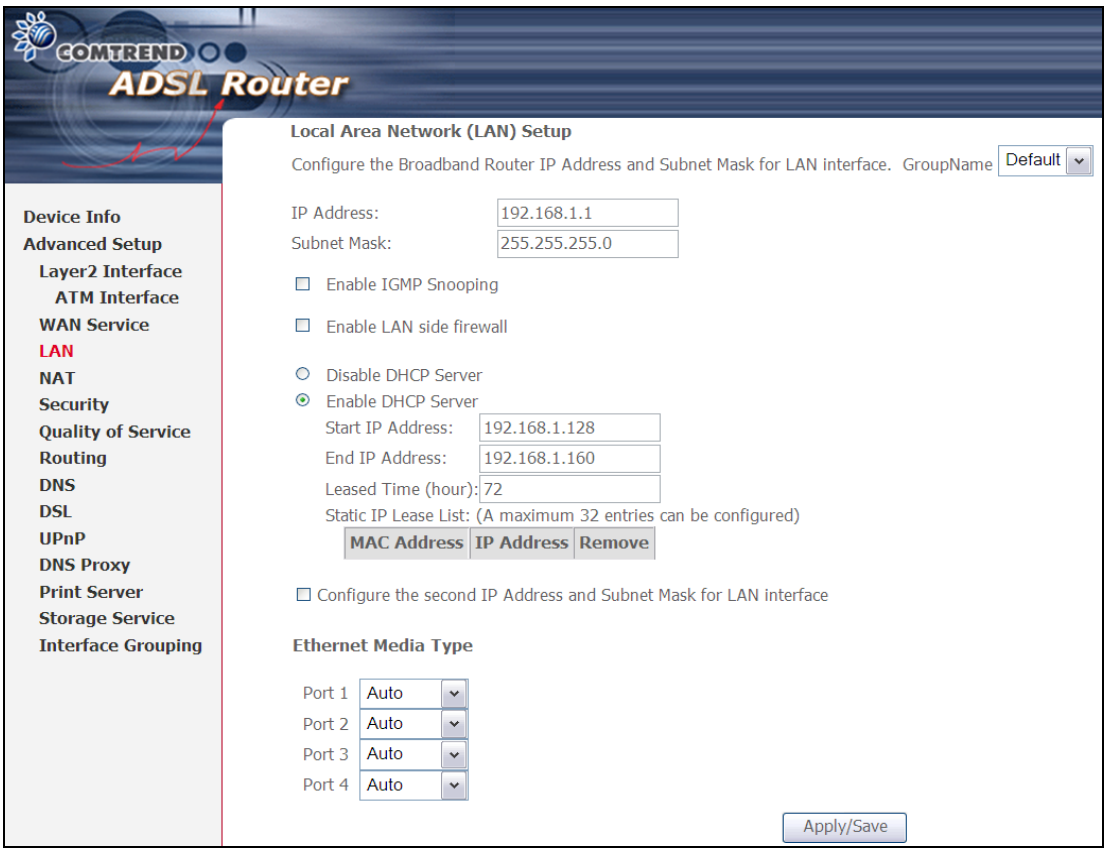
Para eliminar una conexión marque la casilla ☑ de la columna Remove y haga clic en **Remove**.

Para añadir una nueva conexión WAN, haga clic sobre el botón **Add** y siga las instrucciones.

NOTA:	Pueden configurarse hasta 8 perfiles PVC y guardarse en la memoria Flash. Tampoco pueden coexistir conexiones de servicio ETH y PTM/ATM.

5.3 LAN

Configure los ajustes de la interfaz LAN y haga clic en **Apply / Save**.



Consulte las descripciones de los campos más abajo para conocer más detalles.

GroupName: Seleccione un grupo de interfaz

1ª INTERFAZ LAN

IP Address: Introduzca la dirección IP para el puerto LAN.

Subnet Mask: Introduzca la máscara de subred para el puerto LAN.

Enable IGMP Snooping: Actívelo marcando la casilla ☑

Standard Mode: En el modo Estándar, el tráfico multidifusión es enviado a todos los puertos en bridge cuando ningún cliente se abona a un grupo multidifusión, incluso si IGMP snooping está activo.

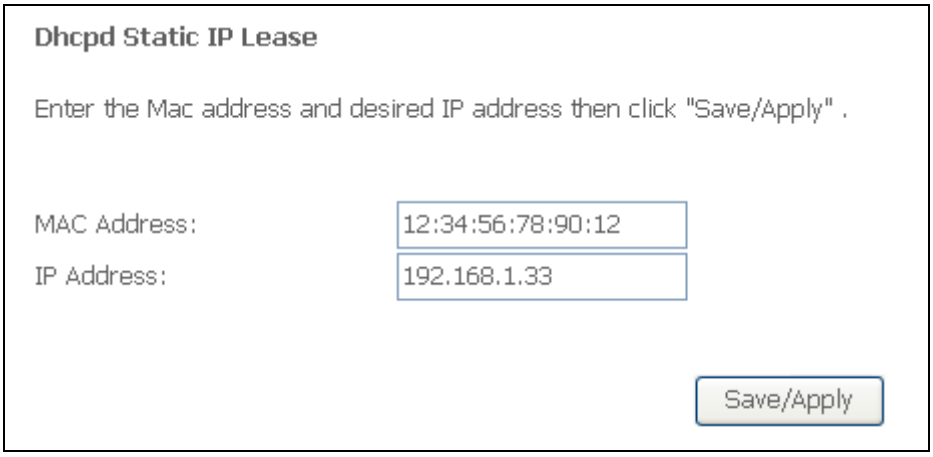
Blocking Mode: En el modo Bloqueo, el tráfico multidifusión se bloqueará y no se dirigirá a los puertos en bridge cuando no hay clientes abonados a algún grupo multidifusión.

Enable LAN side firewall: Actívelo marcando la casilla ☑

DHCP Server: Para activar DHCP seleccione **Enable DHCP server** e introduzca las direcciones IP de Inicio y Fin y el tiempo de Abonado o concesión. Este ajuste configura el router para asignar de forma automática direcciones IP, pasarela por defecto y servidor DNS a cada PC de su LAN.

Static IP Lease List: Pueden configurarse un máximo de 32 entradas.

Para añadir una entrada introduzca la dirección MAC y la IP estática y haga clic sobre **Save / Apply**.

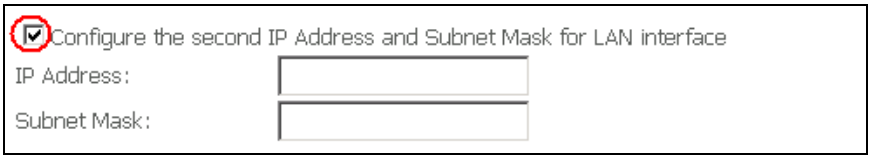


Para eliminar una entrada haga clic en la casilla correspondiente ☑ de la columna Remove y luego haga clic sobre el botón **Remove Entries** como se muestra debajo.

DHCP Server Relay: Actívelo mediante la casilla ☑ e introduzca la dirección IP del servidor DHCP. Permite al router reenviar los paquetes DHCP al servidor remoto DHCP. El servidor remoto proporcionará la dirección IP. ***Esta opción permanece oculta si NAT está activo o si el router está configurado con un único PVC Bridge.***

2ª INTERFAZ LAN

Para configurar una dirección IP secundaria marque la casilla ☑ resaltada en ROJO en la imagen inferior.



IP Address: Introduzca la dirección IP para el puerto LAN.

Subnet Mask: Introduzca la máscara de subred secundaria para el puerto LAN.

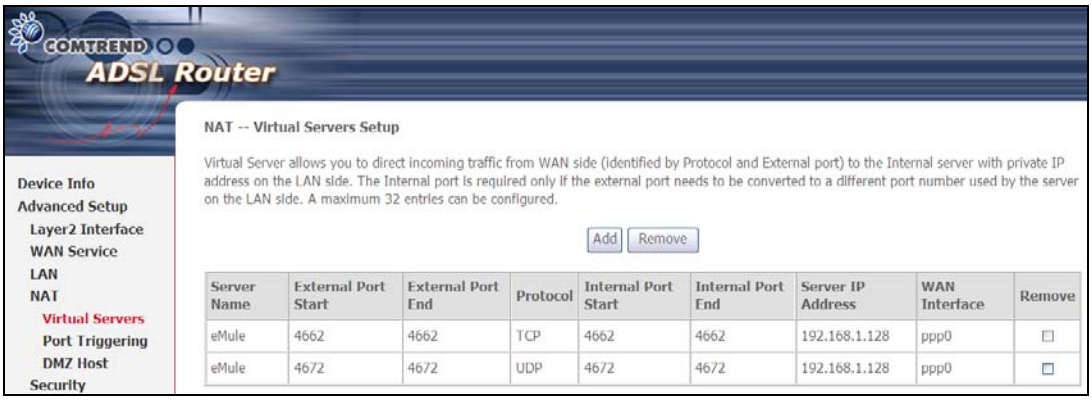
Ethernet Media Type: Para cada puerto Ethernet seleccione entre las opciones Auto, 10_Half, 10_Full, 100_Half ó 100_Full.

5.4 NAT

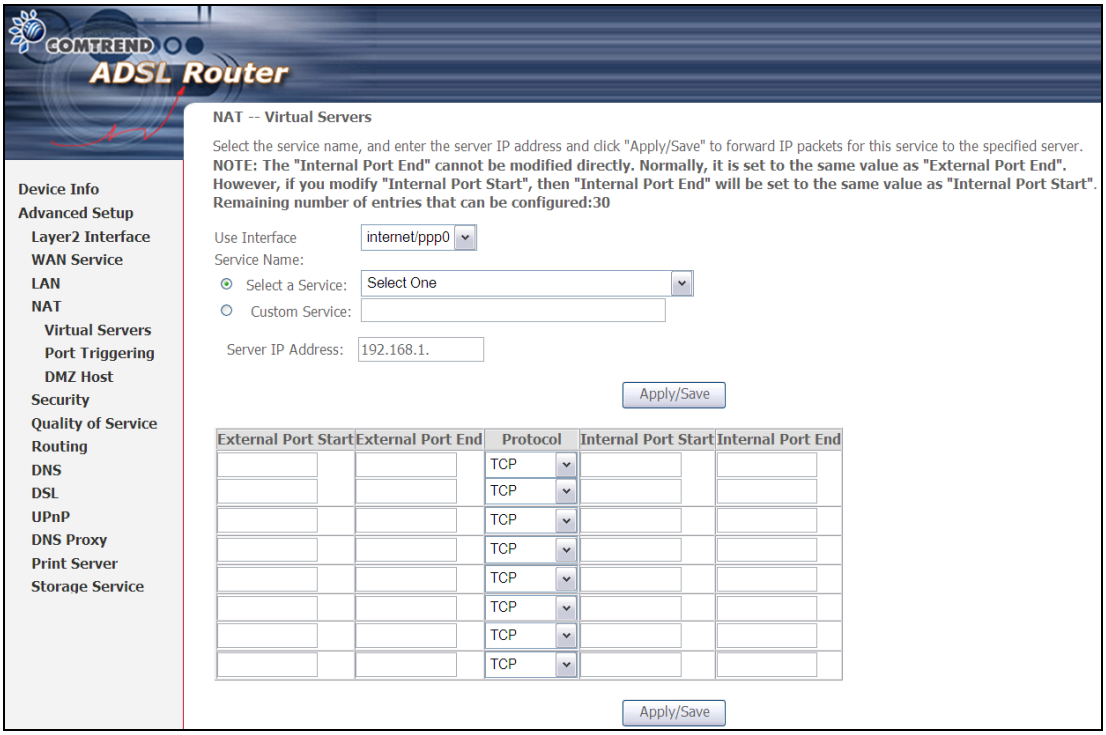
Para ver esta opción, NAT debe estar activado en al menos una conexión PVC mostrada en la pantalla Capítulo 5 Configuración avanzada. NAT no se encuentra disponible como opción en el modo Bridge.

5.4.1 Virtual Servers (Servidores virtuales)

Virtual Servers le permite dirigir el tráfico entrante desde el entorno de la WAN (identificado por Protocol y External port) al servidor interno con la dirección IP privada en el entorno de la LAN. El puerto interno solamente es requerido si el puerto externo necesita convertirse en un número distinto del puerto usado por el servidor en el entorno de la LAN.
Pueden configurarse un máximo de 32 entradas.



Para añadir un servidor virtual, simplemente haga clic en el botón **Add**. Se mostrará la siguiente pantalla.

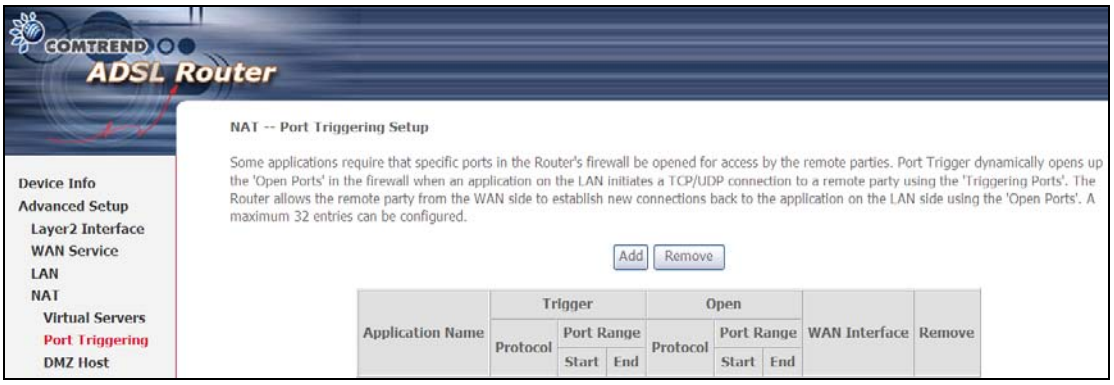


Consulte los campos y su descripción en la tabla inferior.

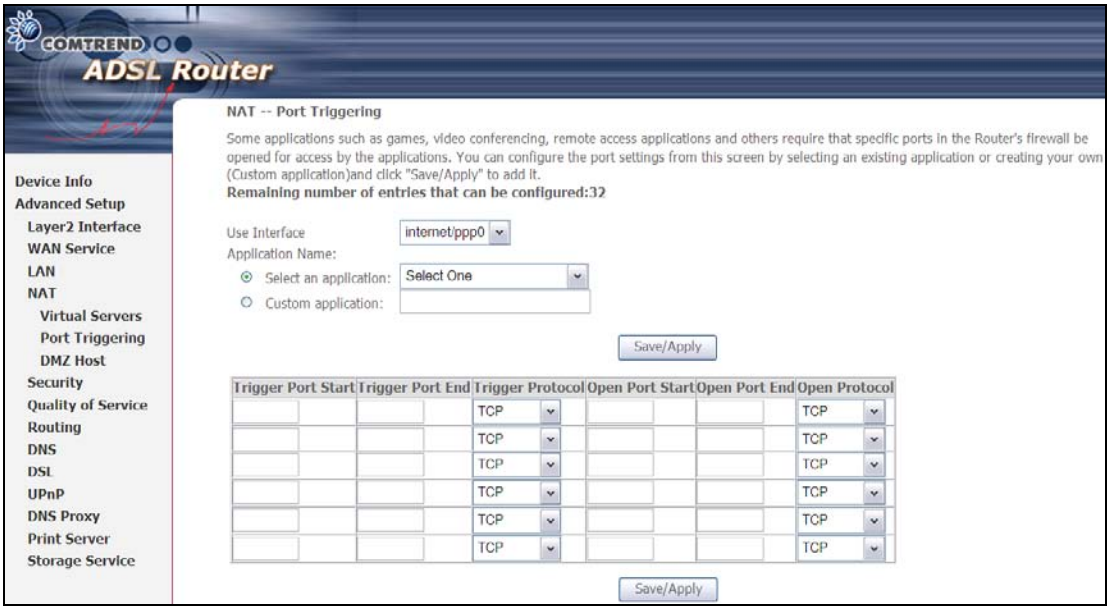
Campo/Encabezado	**Descripción**
Use Interface	Seleccione una interfaz WAN desde la caja desplegable.
Select a Service **Or** Custom Service	El usuario seleccionará un servicio de la lista. **O** El usuario puede escribir un nombre de su elección.
Server IP Address	Introduzca la dirección IP del servidor.
External Port Start	Introduzca el número del puerto externo inicial (cuando seleccione Custom Server). Cuando se selecciona un servicio el rango de puertos se configura de forma automática.
External Port End	Introduzca el número del puerto externo final (cuando seleccione Custom Server). Cuando se selecciona un servicio el rango de puertos se configura de forma automática.
Protocol	El usuario puede seleccionar TCP, TCP/UDP o UDP.
Internal Port Start	Introduzca el número del puerto interno inicial (cuando seleccione Custom Server). Cuando se selecciona un servicio el rango de puertos se configura de forma automática.
Internal Port End	Introduzca el número del puerto interno final (cuando seleccione Custom Server). Cuando se selecciona un servicio el rango de puertos se configura de forma automática.

5.4.2 Port Triggering (Redireccionamiento de puertos)

Algunas aplicaciones requieren que se abran en el firewall puertos específicos para que se pueda acceder a ellos de forma remota. La función “Port Triggering” abre dinámicamente los puertos especificados en el firewall cuando una aplicación de la LAN inicia una conexión TCP/UDP a un grupo remoto utilizando “Triggering Ports” (redireccionamiento de puertos). El router permite al grupo o cliente remoto del entorno de la WAN establecer conexiones nuevas con la aplicación del entorno de la LAN mediante los “puertos abiertos”. Pueden configurarse un máximo de 32 entradas.


COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
NAT
Virtual Servers
Port Triggering
DMZ Host
NAT -- Port Triggering Setup
Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.
Add
Remove
Application Name
Trigger
Protocol
Port Range
Start
End
Open
Protocol
Port Range
Start
End
WAN Interface
Remove

Para añadir un Trigger Port (puerto redirigido), haga clic en el botón **Add**. Se mostrará la siguiente pantalla.



Consulte los campos y su descripción en la tabla inferior.

Campo/Encabezado	Descripción
Use Interface	Seleccione una interfaz WAN en la lista desplegable.
Select an Application **Or** Custom Application	El usuario seleccionará una aplicación de la lista. **O** El usuario puede escribir un nombre de su elección.

Campo / Encabezado	Descripción
Trigger Port Start	Introduzca el número del Trigger Port inicial (cuando seleccione Custom Application). Cuando se selecciona una aplicación el rango de puertos se configura de forma automática.
Trigger Port End	Introduzca el número del Trigger Port final (cuando seleccione Custom Aplication). Cuando se selecciona una aplicación el rango de puertos se configura de forma automática.
Trigger Protocol	El usuario puede seleccionar TCP, TCP/UDP, o UDP.
Open Port Start	Introduzca el número de Puerto Abierto inicial (cuando seleccione Custom Aplication). Cuando se selecciona una aplicación el rango de puertos se configura de forma automática.
Open Port End	Introduzca el número de Puerto Abierto final (cuando seleccione Custom Aplication). Cuando se selecciona una aplicación el rango de puertos se configura de forma automática.
Open Protocol	El usuario puede seleccionar TCP, TCP/UDP, o UDP.

5.4.3 DMZ Host

El router DSL enviará desde la WAN al DMZ host los paquetes IP que no pertenezcan ninguna de las aplicaciones configuradas en la tabla de servidores virtuales.

COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
NAT
Virtual Servers
Port Triggering
DMZ Host
NAT -- DMZ Host
The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.
Enter the computer's IP address and click 'Apply' to activate the DMZ host.
Clear the IP address field and click 'Apply' to deactivate the DMZ host.
DMZ Host IP Address:
Save/Apply

Para Activar el DMZ host, introduzca la dirección IP del DMZ host y haga clic sobre **Save / Apply**.

Para Desactivar el DMZ host, borre la dirección IP del campo y haga clic sobre **Save / Apply**.

5.5 Seguridad

Para ver esta función debe habilitar la característica de firewall (cortafuegos) en la configuración WAN.
Para ver una descripción más detallada con ejemplos consulte el Apéndice A – Firewall (Cortafuegos) .

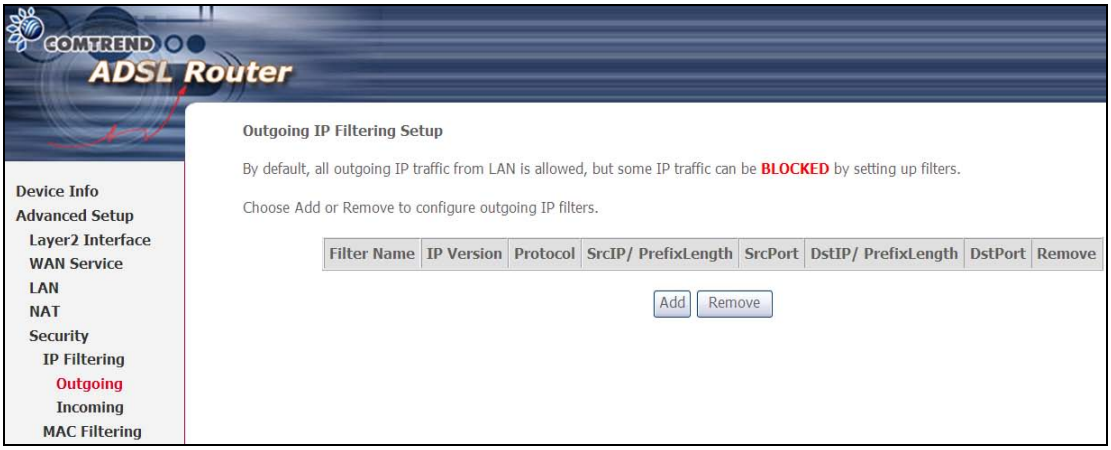
5.5.1 IP Filtering (Filtrado IP)

Esta pantalla permite crear reglas de filtrado que limitan el tráfico IP (salida/entrada). Pueden definirse múltiples reglas de filtrado y cada una establece al menos una condición de limitación. Para que los paquetes IP individuales pasen el filtro deben cumplirse todas las condiciones.

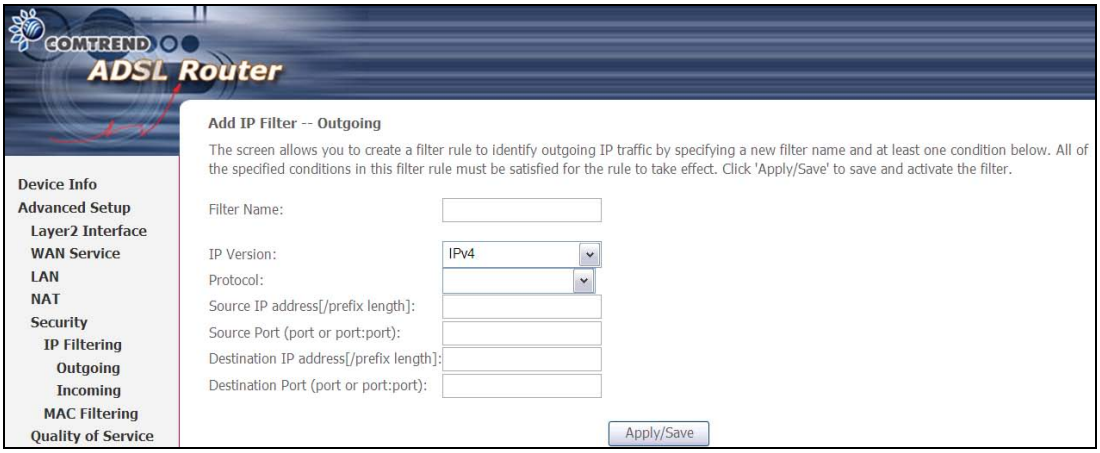
NOTA:	Esta función no está disponible cuando se trabaja en modo Bridge. En su lugar, la opción 5.5.2 MAC Filtering (Filtrado MAC) realiza una función similar.

OUTGOING IP FILTER (Filtro IP de salida)

Por defecto todo el tráfico IP de salida está permitido, pero puede bloquearse con la utilización de filtros.



Para añadir un filtro, es decir, para bloquear el tráfico IP de salida, haga clic sobre el botón **Add**.
En la siguiente pantalla, introduzca su criterio de filtrado y seguidamente haga clic en **Apply / Save**.


COMTREND
ADSL Router
Add IP Filter -- Outgoing
The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
NAT
Security
IP Filtering
Outgoing
Incoming
MAC Filtering
Quality of Service
Filter Name:
IP Version:
IPv4
Protocol:
Source IP address[/prefix length]:
Source Port (port or port:port):
Destination IP address[/prefix length]:
Destination Port (port or port:port):
Apply/Save

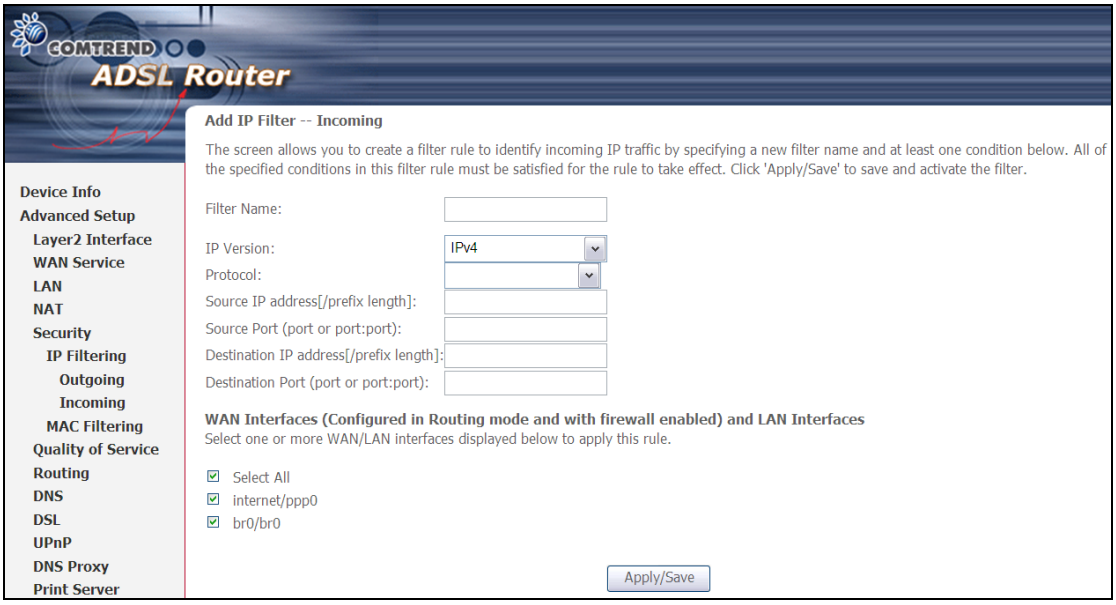
Consulte descripciones de los campos en la tabla inferior.

Campo	Descripción
Filter Name	Escriba un nombre para la regla de filtrado.
IP Version	Seleccionada la versión IPv4 por defecto.
Protocol	El usuario puede seleccionar TCP, TCP/UDP, UDP. O ICMP.
Source IP address	Introduzca la dirección IP de origen.
Source Port (port or port:port)	Introduzca el número o rango de puertos de origen.
Destination IP address	Introduzca la dirección IP de destino.
Destination Port (port or port:port)	Introduzca el número o rango de puertos de destino.

INGOING IP FILTER (Filtro IP de entrada)

Por defecto todo el tráfico IP de entrada está bloqueado, pero ese tráfico puede permitirse con la utilización de filtros.

Para añadir un filtro que permita el tráfico IP de entrada, haga clic sobre el botón **Add**.
En la siguiente pantalla, introduzca su criterio de filtrado y seguidamente haga clic en **Apply / Save**.



Consulte las descripciones de los campos en la tabla inferior.

Campo	Descripción
Filter Name	Escriba un nombre para la regla de filtrado.
IP Version	Seleccionada la versión IPv4 por defecto.
Protocol	El usuario puede seleccionar TCP, TCP/UDP, UDP. O ICMP.
Source IP address	Introduzca la dirección IP de origen.
Source Port (port or port:port)	Introduzca el número o rango de puertos de origen.
Destination IP address	Introduzca la dirección IP de destino.
Destination Port (port or port:port)	Introduzca el número o rango de puertos de destino.

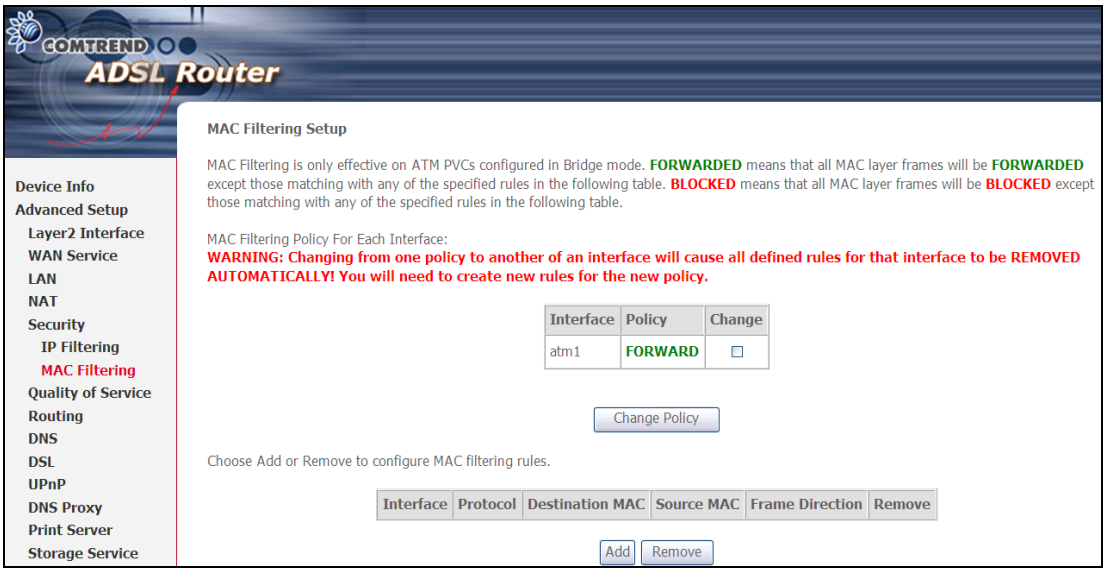
En la parte inferior de esta pantalla, seleccione las interfaces WAN y LAN a las que se aplica la regla de filtrado. Puede seleccionar todas o simplemente un subconjunto de ellas. Las interfaces WAN en modo bridge o sin el firewall activo no estarán disponibles.

5.5.2 MAC Filtering (Filtrado MAC)

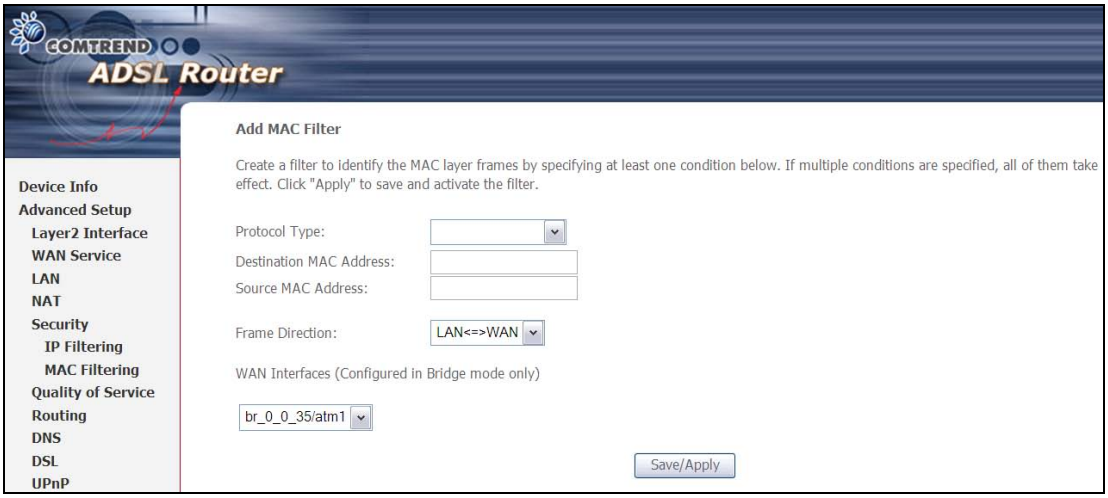
NOTA:	Esta opción está únicamente disponible cuando se trabaja en modo Bridge. Otros modos usan 5.5.1 IP Filtering (Filtrado IP) para realizar una función similar.

Cada dispositivo de red posee una única dirección MAC de 48 bits. Puede usarse para filtrar (bloquear o dejar pasar) los paquetes basándose en el dispositivo de origen. La política de filtrado de MAC y sus reglas para el AR-5387un pueden establecerse de acuerdo con el siguiente procedimiento.

La política global de filtrado MAC se define como sigue. La política **FORWARDED** significa que todas las tramas de capa MAC serán **REENVIADAS** (FORWARDED) excepto aquellas que se ajusten a cualquiera de las reglas especificadas en la tabla siguiente. La política **BLOCKED** significa que todas las tramas de capa MAC serán **BLOQUEADAS** (BLOCKED) excepto aquellas que se ajusten a cualquiera de las reglas especificadas en la tabla siguiente. La opción por defecto es **FORWARDED**. Puede cambiarlo haciendo clic en el botón **Change Policy**.


COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
NAT
Security
IP Filtering
MAC Filtering
Quality of Service
Routing
DNS
DSL
UPnP
DNS Proxy
Print Server
Storage Service
MAC Filtering Setup
MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.
MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.
Interface
Policy
Change
atm1
FORWARD
Change Policy
Choose Add or Remove to configure MAC filtering rules.
Interface
Protocol
Destination MAC
Source MAC
Frame Direction
Remove
Add
Remove

Escoja **Add** o **Remove** para configurar las reglas de filtrado MAC. La siguiente pantalla aparece cuando hace clic en **Add**. Cree un filtro para identificar las tramas de capa MAC especificando al menos una condición. Si se especifican múltiples condiciones, todas ellas deben ser compatibles. Haga clic en **Save / Apply** para guardar y activar el filtro.



Consulte descripciones de los campos en la tabla inferior.

Campo	Descripción
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Define la dirección MAC de destino
Source MAC Address	Define la dirección MAC de origen
Frame Direction	Seleccione la interfaz de paquete entrante/saliente
WAN Interfaces	Aplica el filtro a la interfaz puente seleccionada

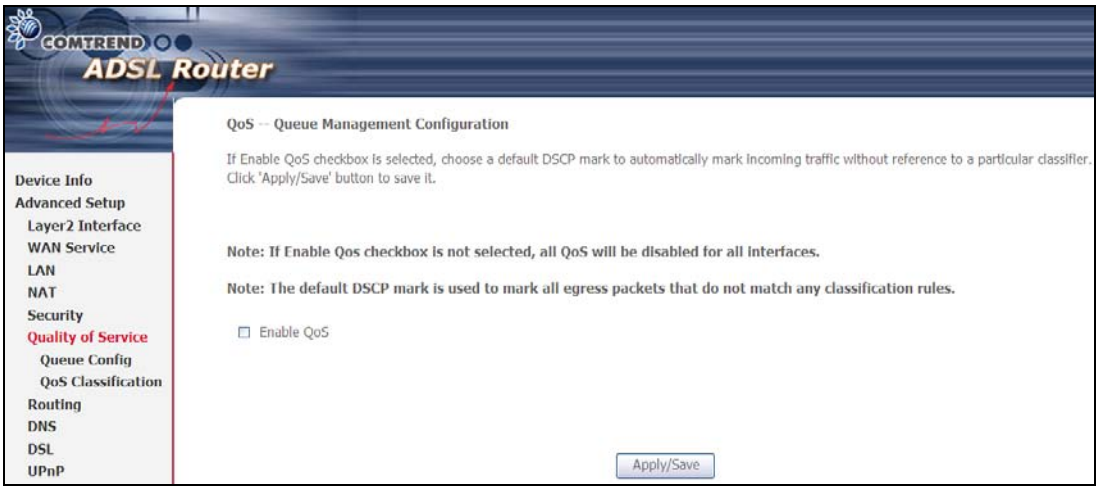
5.6 QoS (Calidad de servicio)

NOTA:	QoS debe activarse en al menos una PVC para que esta opción aparezca. (Véase el Apéndice G – Instalación de la conexión para saber más detalles sobre las instrucciones de configuración de PVC).

5.6.1 Queue Management Configuration (Configuración de gestión de la cola)

Para activar QoS marque la casilla ☑ y seleccione un Default DSCP Mark.

Haga clic sobre **Apply / Save** para activar QoS.


COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
NAT
Security
Quality of Service
Queue Config
QoS Classification
Routing
DNS
DSL
UPnP
QoS -- Queue Management Configuration
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier.
Click 'Apply/Save' button to save it.
Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.
Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.
Enable QoS
Apply/Save

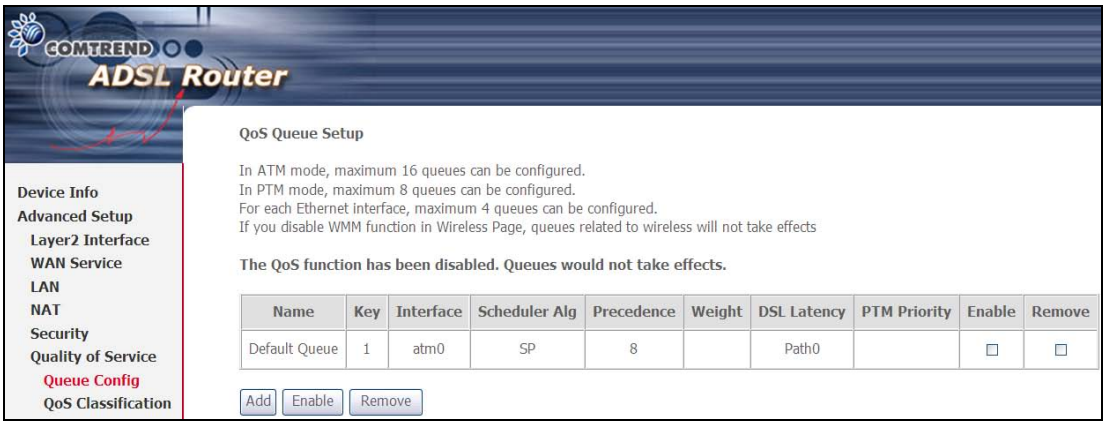
QoS y DSCP Mark se definen como sigue:

Quality of Service (QoS) (Calidad de servicio): Proporciona diferentes prioridades a los distintos usuarios o al flujo de datos, o garantiza un determinado nivel de rendimiento en el flujo de datos de acuerdo con la priorización de las colas.

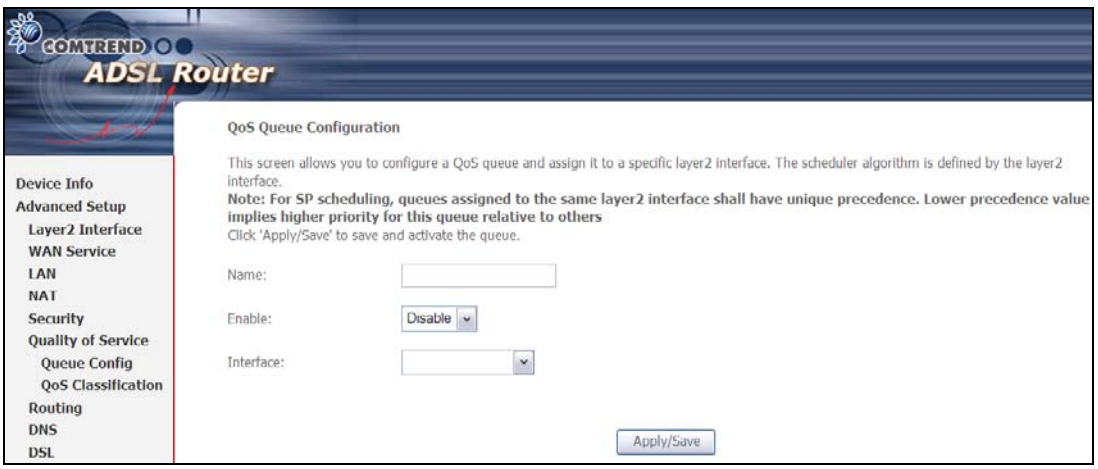
Default Differentiated Services Code Point (DSCP) Mark: Especifica el comportamiento por saltos para un flujo de paquetes dado en el encabezamiento IP (Protocolo de Internet) que no se ajuste con ninguna otra regla de QoS.

5.6.2 Queue Configuration (Configuración de la cola)

Esta función sigue la regla Differentiated Services (Servicios Diferenciados) de QoS IP. Puede crear una nueva entrada de cola haciendo clic sobre el botón **Add**. Active y asigne una interfaz y una precedencia en la siguiente pantalla. Haga clic sobre **Apply / Save** para activarla.



Haga clic sobre **Enable** para activar la cola de QoS. Haga clic sobre **Add** para ver la siguiente pantalla.



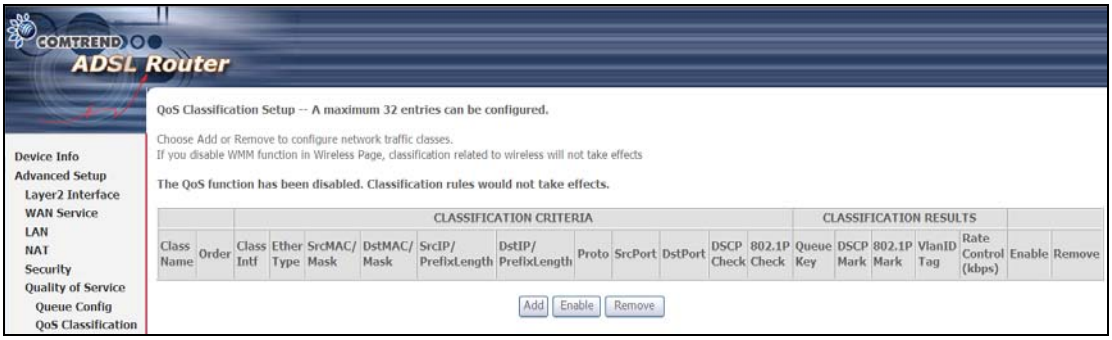
Name: Identificador para la entrada de esta Cola.

Enable: Activa /Desactiva la entrada en la Cola.

Interface: Asigna la entrada a una interfaz de red específica (QoS Activado).

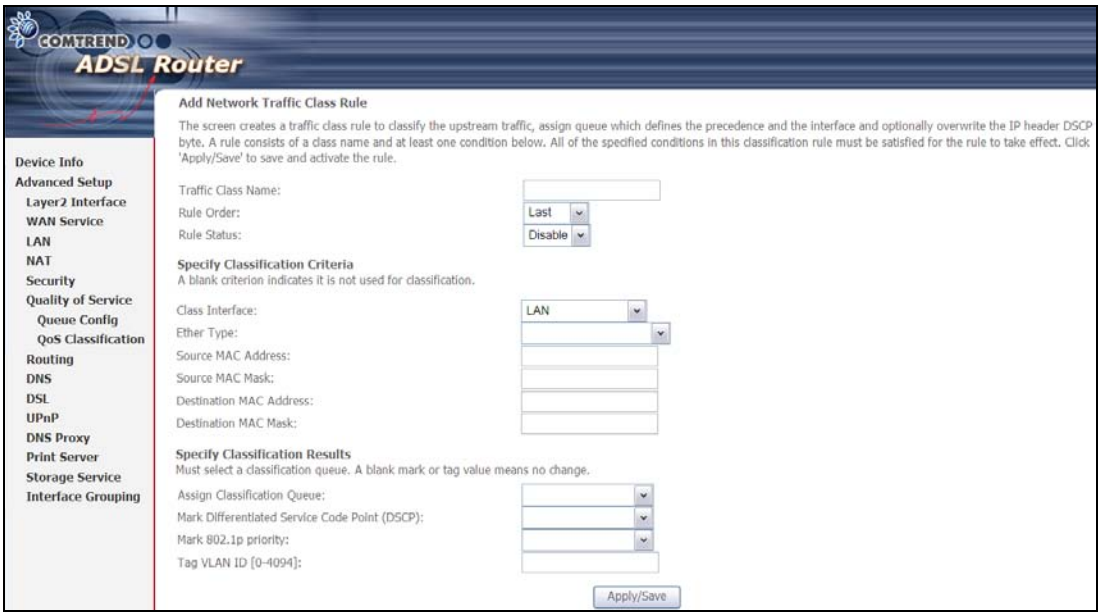
5.6.3 QoS Classification (Clasificación de QoS)

Los tipos de tráfico de la red se describen en la siguiente tabla.



Haga clic sobre **Add** para configurar una regla de tipo de tráfico de la red y sobre **Enable** para activarla. Para eliminar una entrada desde la lista haga clic en **Remove**.

Esta pantalla crea una regla de tipo de tráfico en la red para clasificar el tráfico ascendente, asignar prioridades de cola y, opcionalmente, sobrescribir el byte DSCP de la cabecera IP. Una regla consiste en un nombre de clase y al menos una condición lógica. Todas las condiciones especificadas en la regla deben ser satisfechas para que tenga efecto.


COMTREND
ADSL Router
Add Network Traffic Class Rule
The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the rule.
Traffic Class Name:
Rule Order:
Last
Rule Status:
Disable
Specify Classification Criteria
A blank criterion indicates it is not used for classification.
Class Interface:
LAN
Ether Type:
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:
Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.
Assign Classification Queue:
Mark Differentiated Service Code Point (DSCP):
Mark 802.1p priority:
Tag VLAN ID [0-4094]:
Apply/Save
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
NAT
Security
Quality of Service
Queue Config
QoS Classification
Routing
DNS
DSL
UPnP
DNS Proxy
Print Server
Storage Service
Interface Grouping

Campo	Descripción
Traffic Class Name	Introduzca un nombre para la clase de tráfico.
Rule Order	Last (última) es la única opción.
Rule Status	Desactivar o activar la regla.
Classification Criteria (Criterio de clasificación)	
Class Interface	Seleccione una interfaz (p.ej. Local, eth0-4, wl0)
Ether Type	Establezca el tipo Ethernet (p. ej. IP, ARP, IPv6).

Campo	Descripción
Source MAC Address	Un paquete pertenece a SET-1 si un AND binario de su dirección MAC de origen con su correspondiente máscara MAC de origen (Source MAC Mask) es igual al AND binario de la máscara MAC de origen y este campo.
Source MAC Mask	Esta es la máscara utilizada para decidir cuantos bits son comprobados en Source MAC Address.
Destination MAC Address	Un paquete pertenecerá a SET-1, si un AND binario de su dirección MAC de Destino con su correspondiente máscara MAC de destino es igual al AND binario de la máscara MAC de destino y este campo.
Destination MAC Mask	Esta es la máscara utilizada para decidir cuantos bits son comprobados en Destination MAC Address.
Classification Results (Resultados de la clasificación)	
Assign Classification Queue	Las configuraciones de la cola se presentan en este formato: "Interfacename&Prece P&Queue Q" donde P y Q son la precedencia y las claves de cola para la interfaz correspondiente como se muestra en el listado de la pantalla de configuración de cola.
Mark Differentiated Service Code Point	El Code Point seleccionado da la prioridad correspondiente a los paquetes que satisfacen la regla.
Mark 802.1p Priority	Seleccione entre 0 y 7. Los valores más bajos tienen la prioridad más alta.
Tag VLAN ID	Introduzca una etiqueta ID VLAN 802.1Q [2-4094]

5.7 Routing

Las siguientes funciones de encaminamiento son accesibles desde este menú: **Default Gateway (Pasarela predeterminada), Static Route (Ruta estática) , Policy Routing (Política de encaminamiento), RIP** and **IPv6 Static Route (Ruta estática IPv6)**.

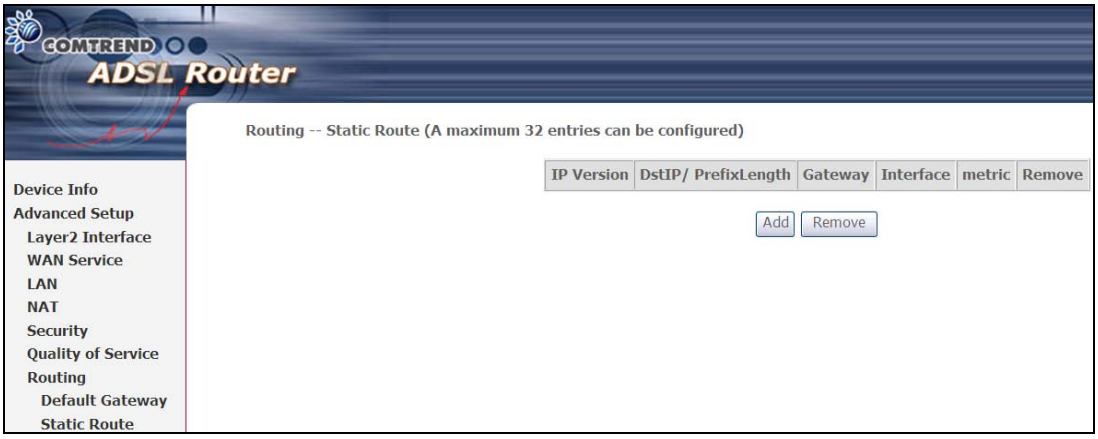
NOTA:	En el modo bridge, la opción de menú **RIP** está oculta, mientras que las otras opciones de menú se muestran aunque no estén operativas.

5.7.1 Default Gateway (Pasarela predeterminada)

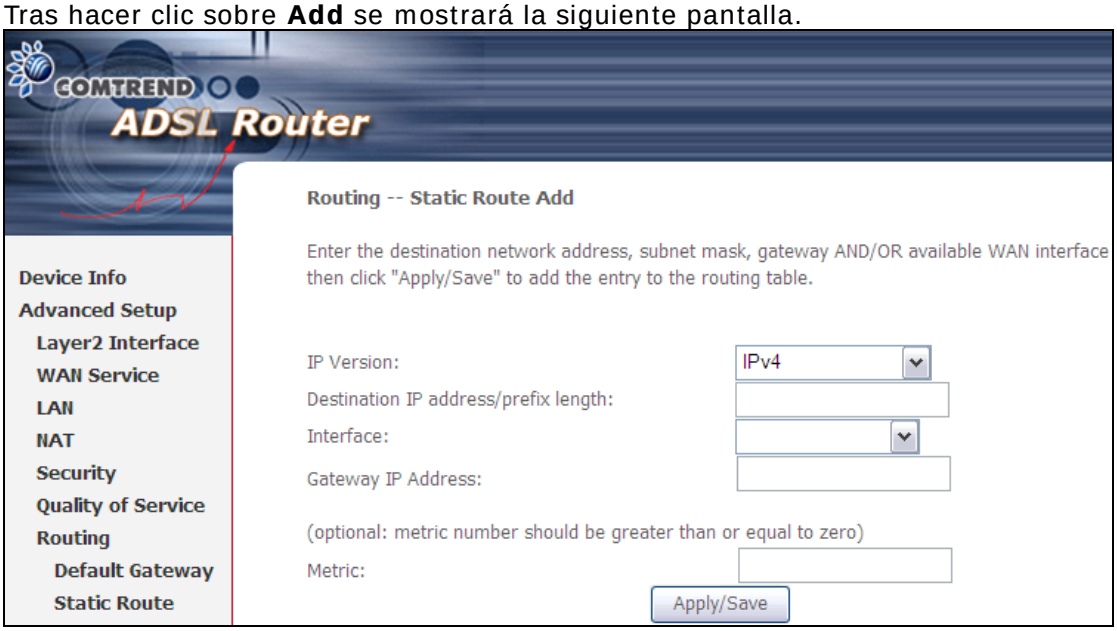
El listado del interfaz de Default gataway puede tener múltiples interfaces WAN que servirán como sistemas default gateway, pero, si la interfaz WAN está conectada, sólo uno de ellos se usará en función de la prioridad que tengan, siendo el primero el de prioridad más alta y el último de prioridad más baja. El orden de prioridad se puede cambiar eliminándolos todos y añadiéndolos de nuevo en el orden deseado.

5.7.2 Static Route (Ruta estática)

Esta opción permite la configuración de rutas estáticas por IP de destino. Haga clic sobre **Add** para crear una ruta estática o clic en **Remove** para eliminarla.



Tras hacer clic sobre **Add** se mostrará la siguiente pantalla.

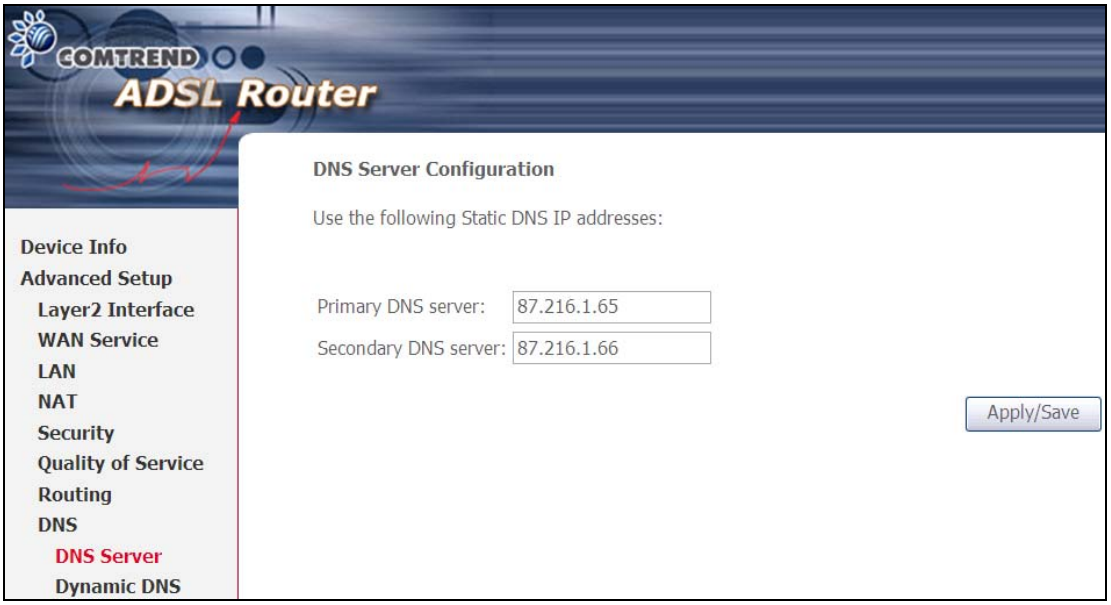


Introduzca la dirección de IP de destino, seleccione el tipo de interfaz, introduzca el IP de la pasarela (Gateway IP) y el Número Métrico si es requerido. A continuación haga clic sobre **Apply/Save** para añadir una nueva entrada a la tabla de encaminamiento.

5.8 DNS

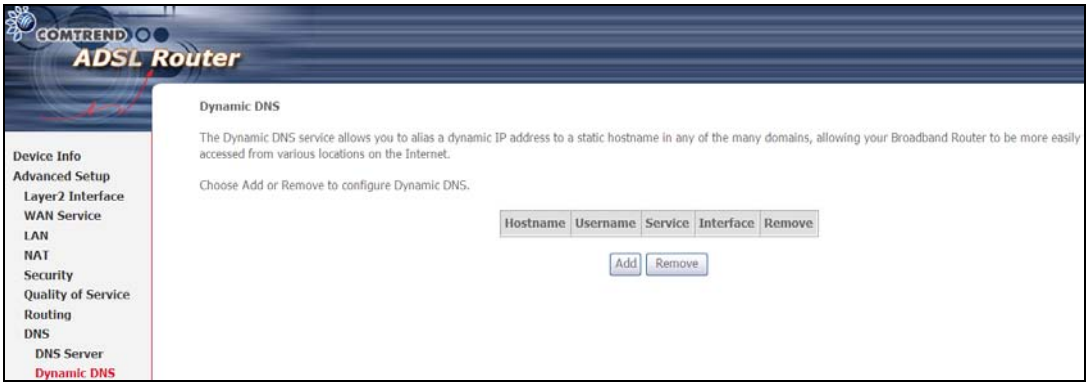
5.8.1 DNS Server (Servidor DNS)

Haga clic sobre **Apply / Save** para guardar la nueva configuración.



5.8.2 Dynamic DNS (DNS Dinámico)

El servicio Dynamic DNS le permite convertir una dirección IP dinámica en el nombre del host estático de cualquiera de los muchos dominios, consiguiendo así que el AR-5387un sea accesible de una forma más fácil desde las distintas localizaciones en Internet.



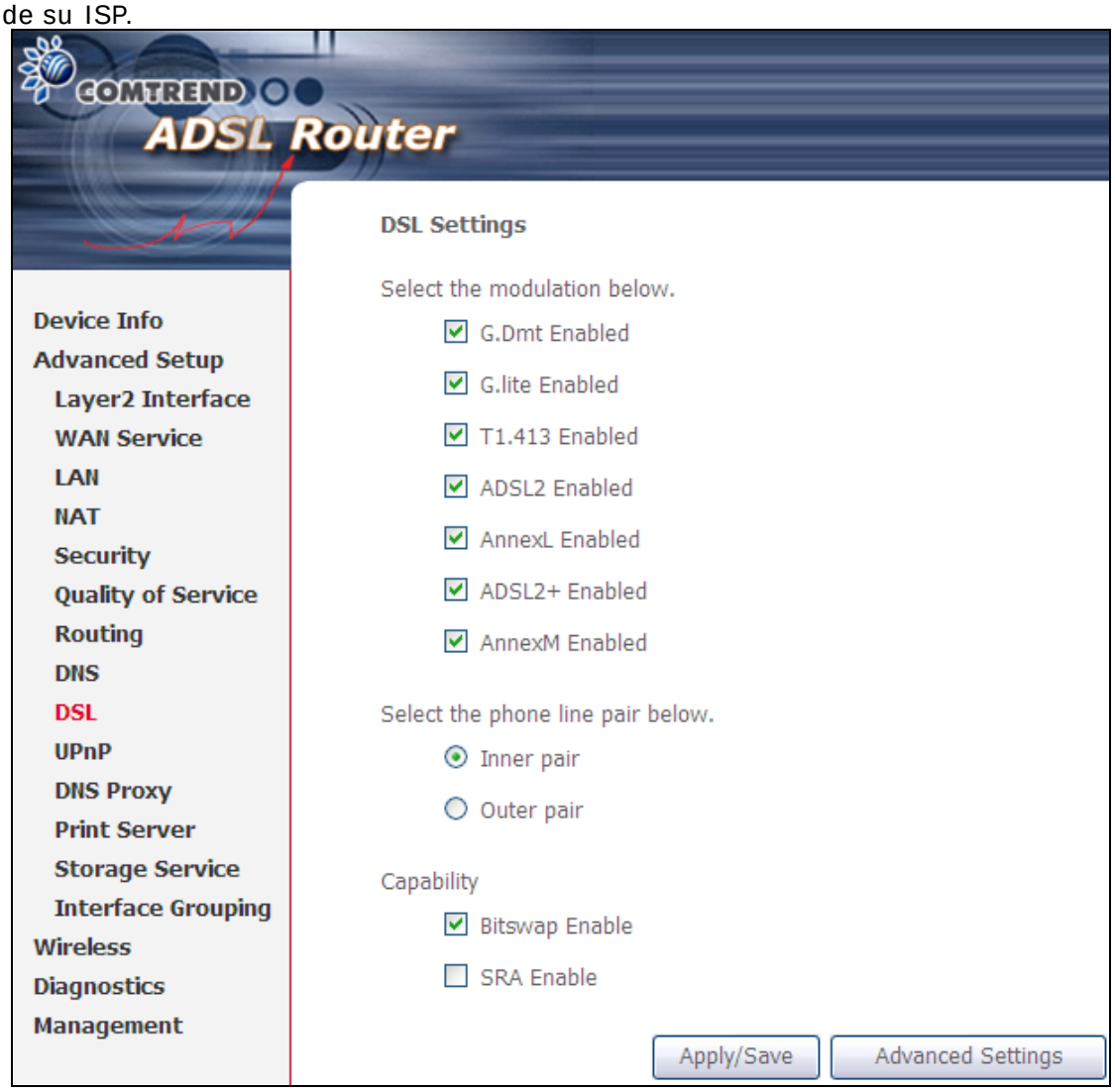
Para añadir un servicio de DNS dinámico, haga clic en el botón **Add**. Se mostrará la siguiente pantalla.

Consulte descripciones de los campos en la tabla inferior.

Campo	Descripción
D-DNS provider	Seleccione un proveedor de DNS dinámico de la lista
Hostname	Introduzca el nombre para el servidor DNS dinámico
Interface	Seleccione la interfaz de la lista
Username	Introduzca el nombre de usuario para el servidor DNS dinámico
Password	Introduzca la contraseña para el servidor DNS dinámico

5.9 DSL

La pantalla DSL Settings (Configuraciones DSL) le permite seleccionar un modo de modulación DSL adecuado.
Para lograr un rendimiento óptimo los modos seleccionados deberían coincidir con los de su ISP.

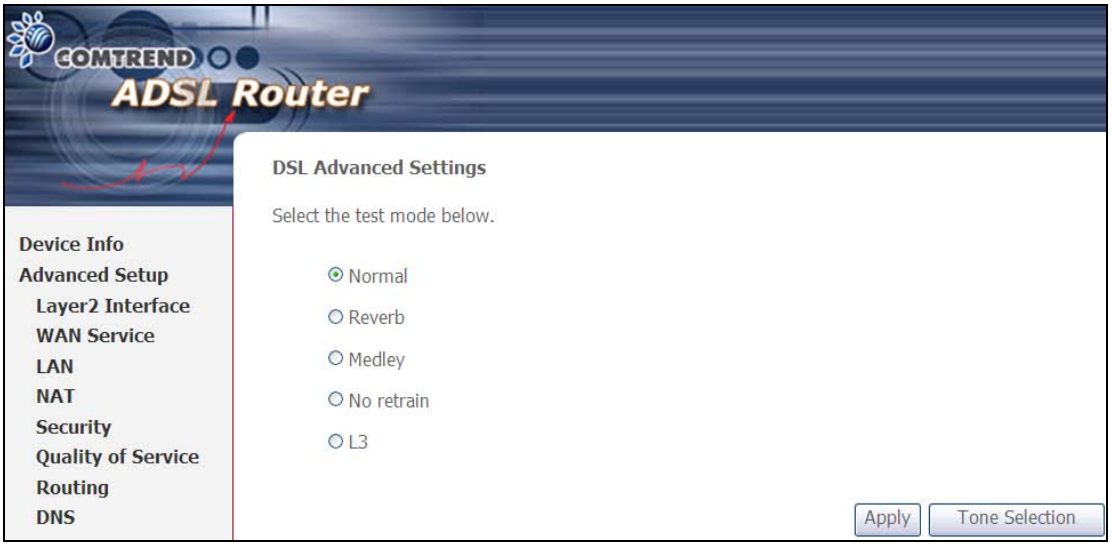


Modo DSL	**Tasa de transmisión de datos - Mbps (Megabits por segundo)**
G.Dmt	Bajada: 12 Mbps Subida: 1,3 Mbps
G.lite	Bajada: 4 Mbps Subida: 0,5 Mbps
T1.413	Bajada: 8 Mbps Subida: 1,0 Mbps
ADSL2	Bajada: 12 Mbps Subida: 1,0 Mbps
AnnexL	Soporta bucles más largos pero con menores tasas de transmisión.
ADSL2+	Bajada: 24 Mbps Subida: 1,0 Mbps
AnnexM	Bajada: 24 Mbps Subida: 3,5 Mbps
Opciones	**Descripción**

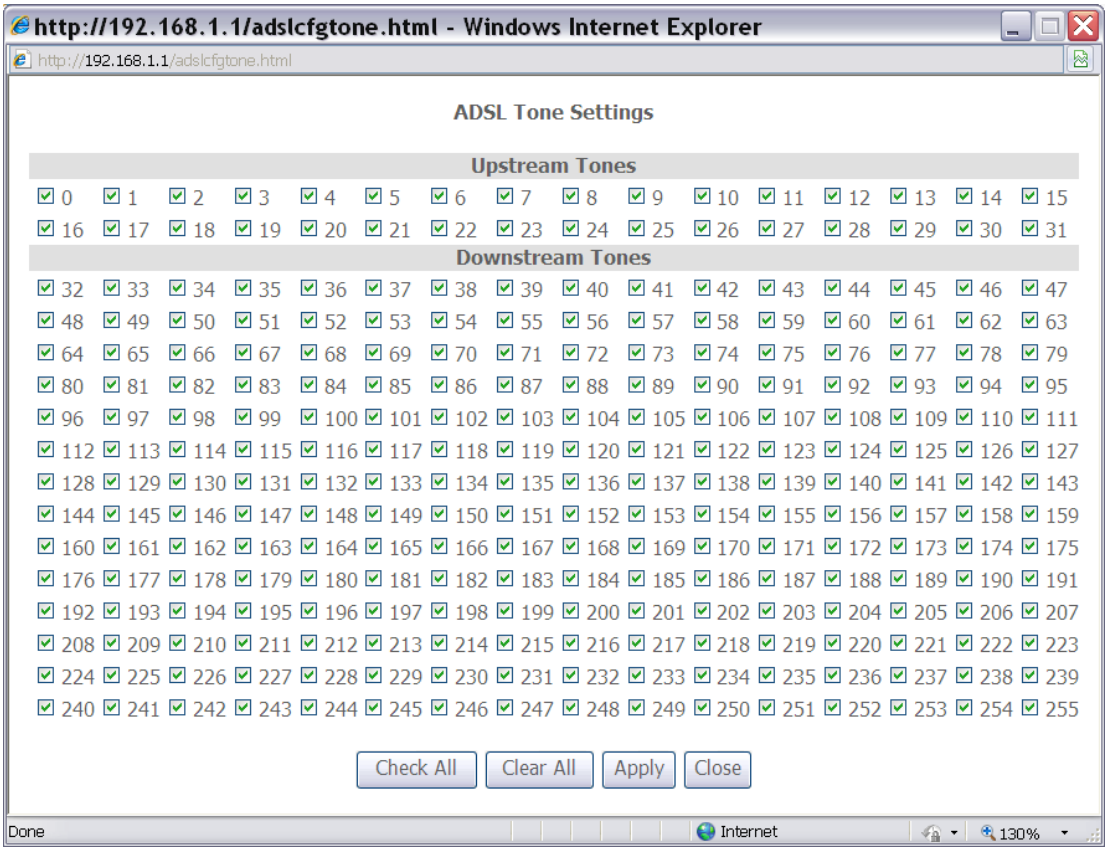
Modo DSL	Tasa de transmisión de datos - Mbps (Megabits por segundo)
Inner/Outer Pair	Selecciona los pin exteriores o interiores del par cruzado (cable RJ11)
Bitswap Enable	Activa la función de handshaking adaptativa bitswap
SRA Enable	Activa la función Seamless Rate Adaptation (SRA)

Advanced DSL Settings (Configuración DLS Avanzada)

Haga clic en **Advanced Settings** para mostrar opciones adicionales. En la siguiente pantalla puede seleccionar un modo de pruebas o modificar los tonos haciendo clic sobre **Tone Selection.** Haga clic en **Apply** para aplicar estos cambios y volver a la pantalla previa.

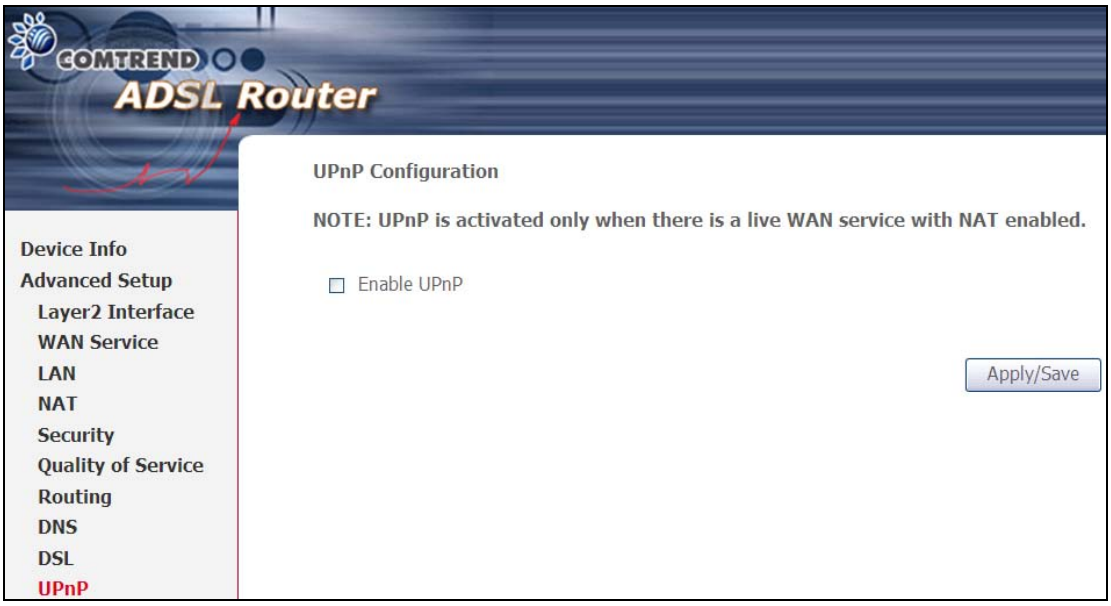


En esta pantalla puede seleccionar los tonos que quiere activar, seguidamente haga clic en **Apply** y **Close**.



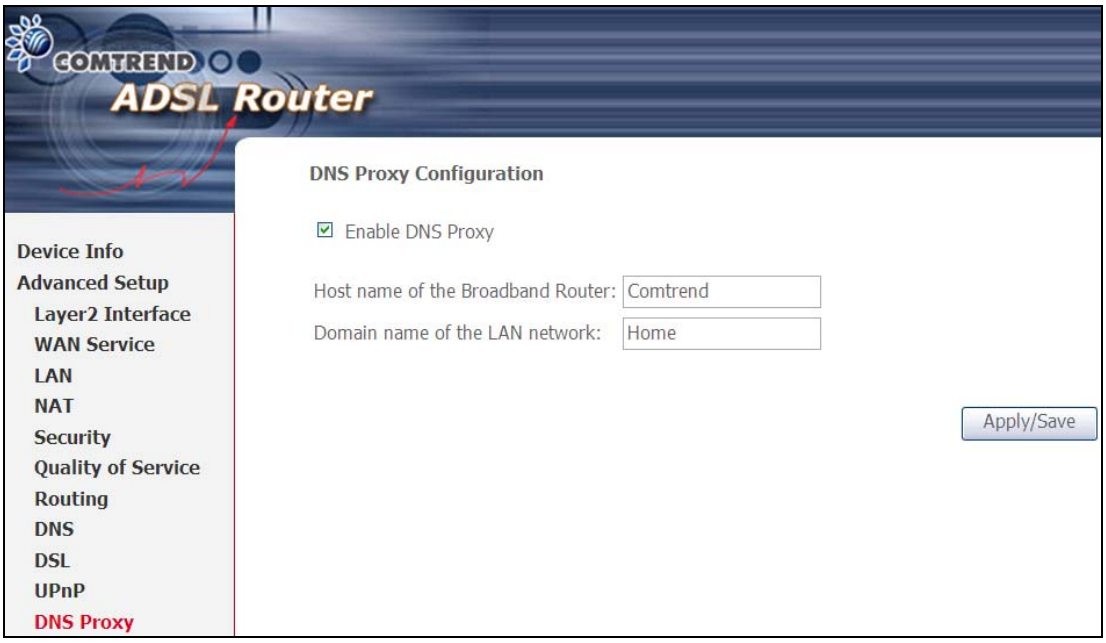
5.10 UPnP

Marque la casilla ☑ dispuesta y haga clic sobre **Apply / Save** para activar el protocolo UPnP.



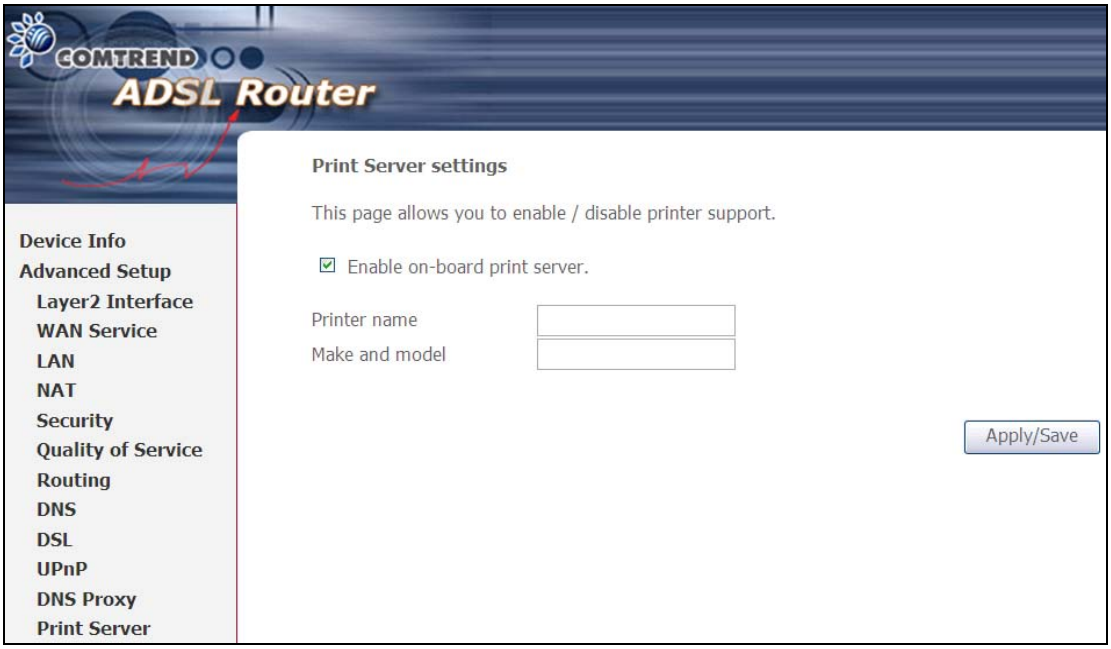
5.11 Proxy DNS

Marque la casilla ☑ dispuesta y haga clic sobre **Apply / Save** para activar.



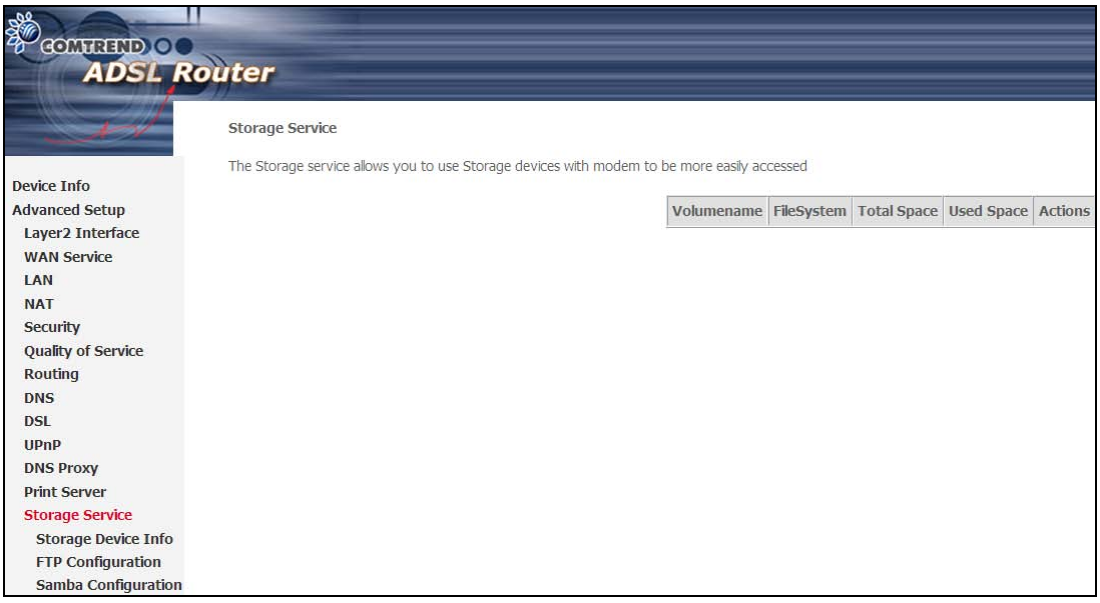
5.12 Servidor de impresión

El AR-5387un puede ofrecer soporte de impresión a través de un Puerto anfitrión USB 2.0 opcional.
Si su dispositivo posee este puerto, vaya al Apéndice F – Servidor de impresión para conocer más detalles de configuración.



5.13 Servicio de almacenamiento

El servicio de almacenamiento le permite usar dispositivos de almacenamiento en el módem de forma que sean fácilmente accesibles.



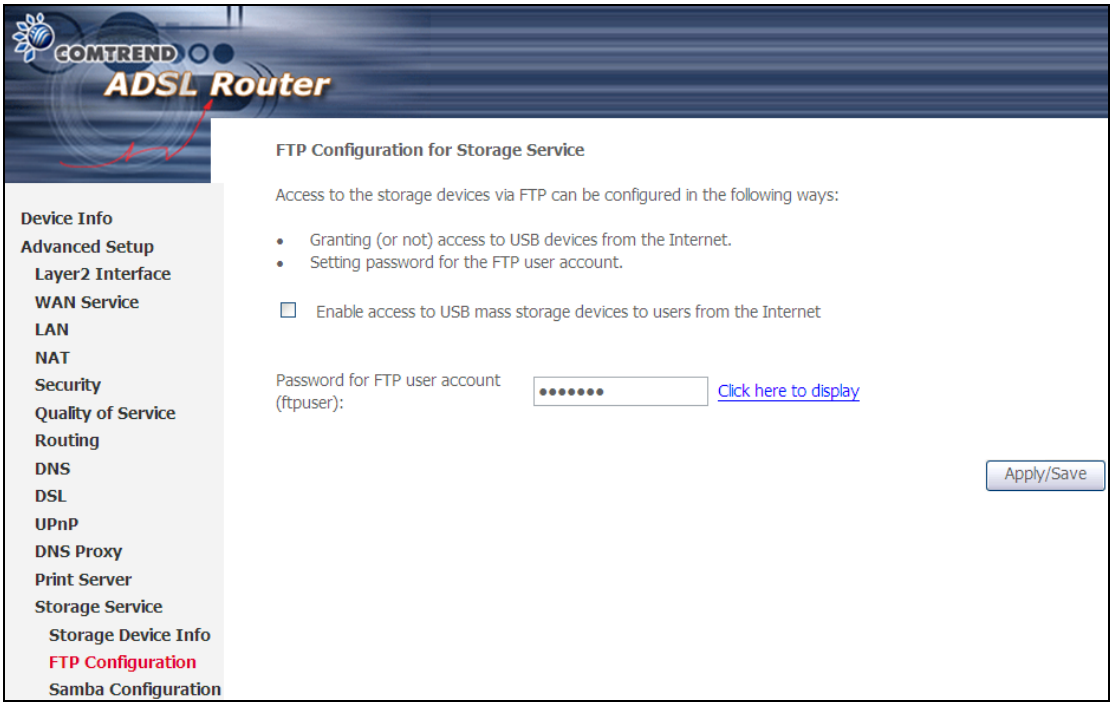
5.13.1 Storage Device Info (Información de Dispositivos de Almacenamiento)

La siguiente pantalla se muestra para su consulta tras acoplar el dispositivo de almacenamiento.

Volumename	FileSystem	Total Space	Used Space	Actions
usb1_1	fat	961	0	Safely remove Explore

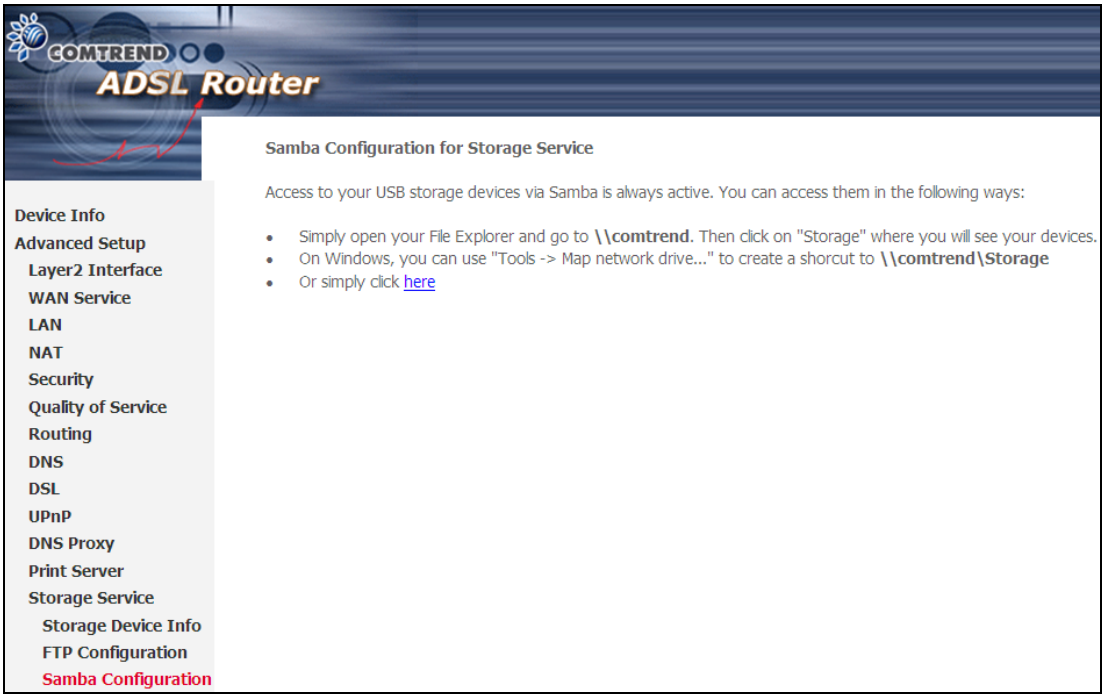
5.13.2 FTP Configuration (Configuración FTP)

Introduzca la contraseña de su cuenta de usuario FTP. El usuario FTP usará la contraseña para acceder al almacenamiento USB compartido.



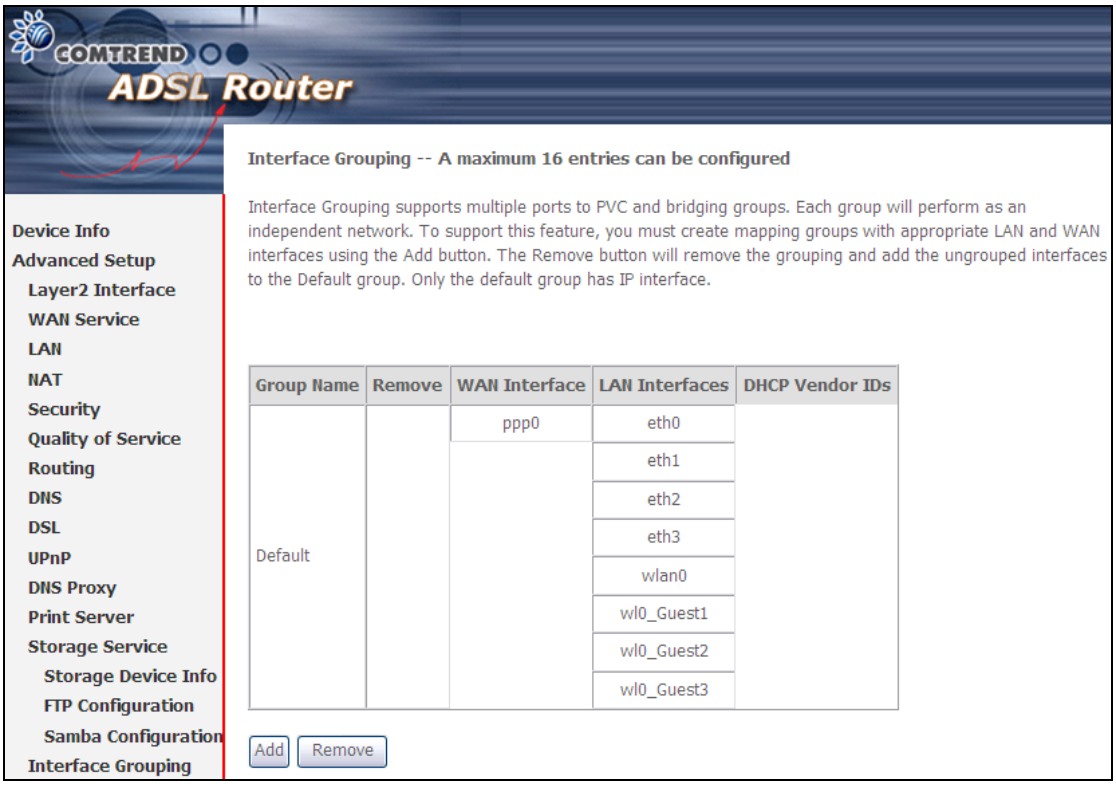
5.13.3 Samba Configuration (Configuración Samba)

Use el protocolo samba para compartir el dispositivo de almacenamiento USB.



5.14 Interface Grouping

Interface Grouping soporta múltiples puertos a grupos PVC y bridging. Cada grupo actúa como una red independiente. Para usar esta función debe crear grupos redirigidos con interfaces LAN y WAN mediante el botón **Add**.
El botón **Remove** elimina los grupos redirigidos, devolviendo las interfaces desagrupadas al grupo Default (Predeterminado). Sólamente el grupo predeterminado tiene una interfaz IP.



Para añadir un Grupo de interfaz haga clic sobre el botón **Add**. Aparecerá la siguiente pantalla. Muestra un listado con las interfaces agrupadas disponibles. Siga las instrucciones que se detallan en la siguiente pantalla.

COMTREND
ADSL Router
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
NAT
Security
Quality of Service
Routing
DNS
DSL
UPnP
DNS Proxy
Print Server
Storage Service
Storage Device Info
FTP Configuration
Samba Configuration
Interface Grouping
Wireless
Diagnostics
Management
Interface grouping Configuration
To create a new interface group:
1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. Note that these clients may obtain public IP addresses
4. Click Apply/Save button to make the changes effective immediately
IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.
Group Name:
WAN Interface used in the grouping
internet/ppp0
Grouped LAN Interfaces
Available LAN Interfaces
eth0
eth1
eth2
eth3
wlan0
wl0_Guest1
wl0_Guest2
wl0_Guest3
->
<-
Automatically Add Clients With the following DHCP Vendor IDs
Apply/Save

Automatically Add Clients With Following DHCP Vendor IDs (Añada clientes automáticamente con los siguientes IDs de proveedor DHCP):

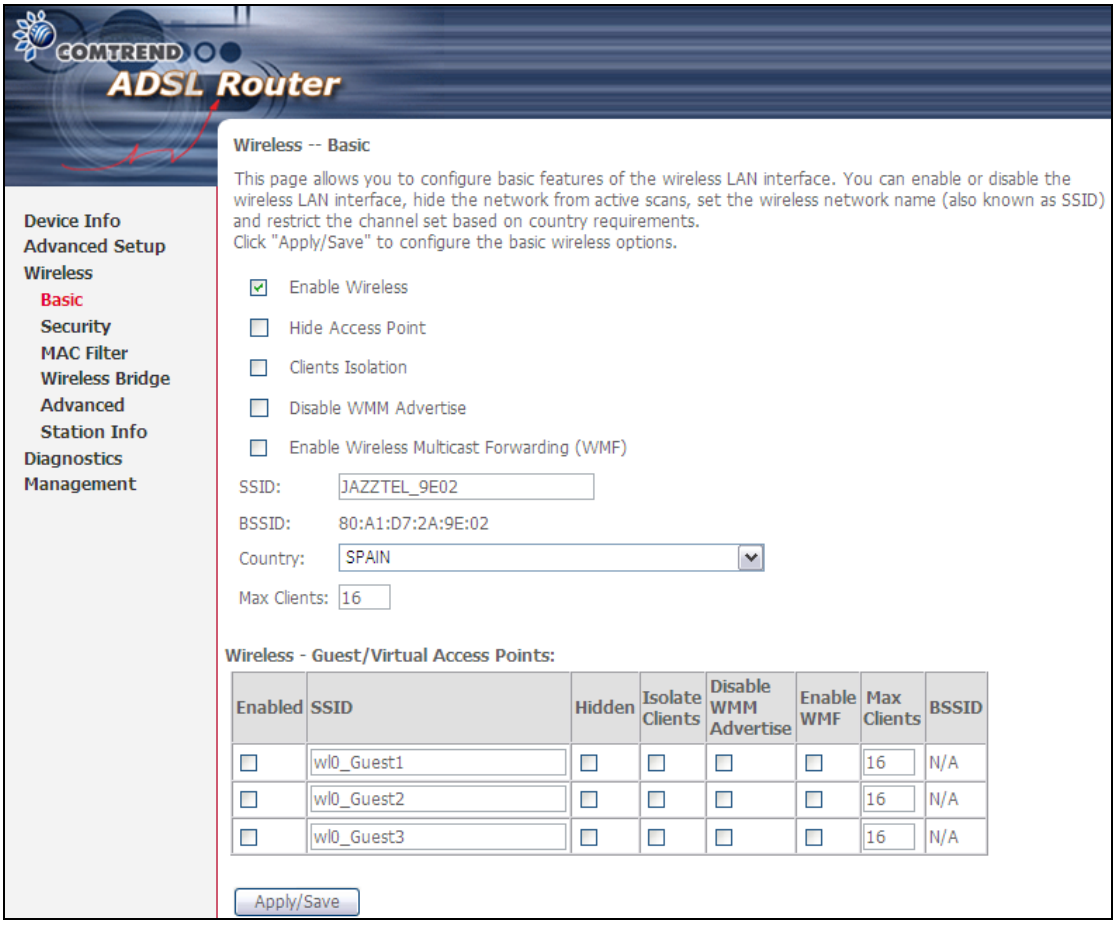
Añade soporte para mapear automáticamente interfaces LAN a los PVCs usando la IP del proveedor DHCP (opción 60). El servidor DHCP local rechazará las peticiones y las reenviará a un servidor DHCP remoto mapeando la interfaz LAN apropiada. Se pone en funcionamiento cuando se activa el Interface Grouping.

Capítulo 6 Función inalámbrica

El menú Wireless proporciona acceso a las opciones inalámbricas que se detallan a continuación.

6.1 Basic (Básico)

La opción **Basic** le permite configurar las propiedades básicas de la interfaz LAN inalámbrica. Se puede activar o desactivar la interfaz LAN inalámbrica, ocultar la red a las búsquedas activas, establecer el nombre de la red inalámbrica (conocido también como SSID) y restringir el conjunto de canales en base a los requisitos de cada país.


COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management
Wireless -- Basic
This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Click "Apply/Save" to configure the basic wireless options.
Enable Wireless
Hide Access Point
Clients Isolation
Disable WMM Advertise
Enable Wireless Multicast Forwarding (WMF)
SSID: JAZZTEL_9E02
BSSID: 80:A1:D7:2A:9E:02
Country: SPAIN
Max Clients: 16
Wireless - Guest/Virtual Access Points:
Enabled SSID Hidden Isolate Clients Disable WMM Advertise Enable WMF Max Clients BSSID
wl0_Guest1 16 N/A
wl0_Guest2 16 N/A
wl0_Guest3 16 N/A
Apply/Save

Haga clic sobre **Apply / Save** para aplicar las opciones inalámbricas seleccionadas.

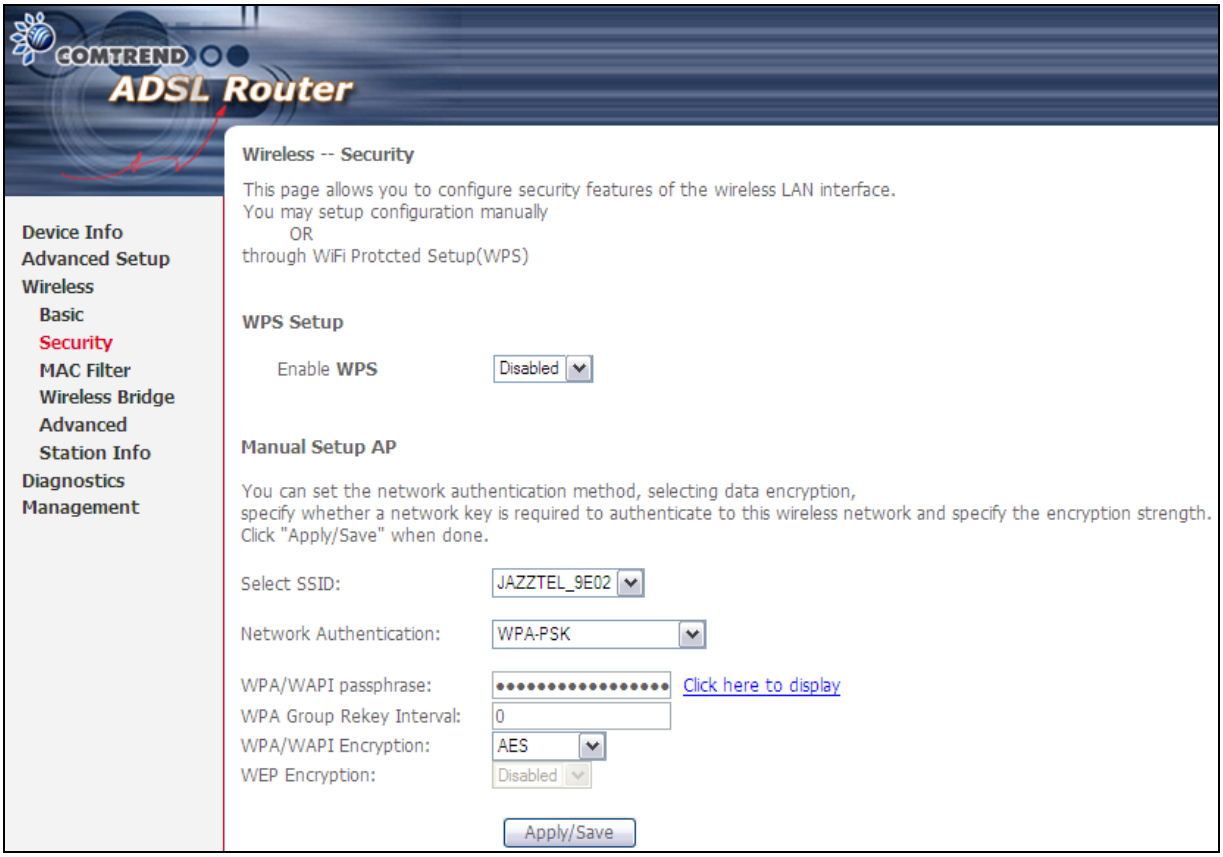
Consulte las descripciones de estas opciones en la tabla inferior.

Opción	Descripción
Enable Wireless	Una casilla ☑ que activa o desactiva la interfaz LAN inalámbrica. Cuando está seleccionada se muestran un conjunto básico de opciones inalámbricas.

Opción	Descripción
Hide Access Point	Seleccione Hide Access Point para que el punto de acceso quede oculto a las búsquedas activas inalámbricas. Para comprobar el estado del punto de acceso (PA) en Windows XP, abra **Network Connections** (Conexiones de red) desde el menú **start** (Inicio) y seleccione **Ver todas las conexiones de red disponibles**. Si el punto de acceso está oculto, no aparecerá en la lista. Para conectar un cliente a un punto de acceso oculto, se debe añadir dicho punto de acceso a la configuración inalámbrica de la estación de forma manual.
Clients Isolation	Cuando está activo se evita que los PCs clientes se vean los unos a los otros en las Conexiones de red o en Mis sitios de red. También evita la comunicación de un cliente inalámbrico con otro.
Disable WMM Advertise	Deja de avisar sobre la funcionalidad Wireless Multimedia (WMM), la cual proporciona una calidad de servicio básica para aplicaciones dependientes del tiempo (como por ejemplo VoIP, Video).
Enable Wireless Multicast Forwarding	Marque la casilla ☑ para activar esta función.
SSID [1-32 characters]	Establece el nombre de la red inalámbrica. SSID corresponde a Service Set Identifier. Todas las estaciones deben estar configuradas con el SSID correcto para acceder a la WLAN. Si el SSID no se corresponde con el de la WLAN, el usuario no podrá tener acceso.
BSSID	El BSSID es una código de identificación de 48 bits que se utiliza para identificar un determinado BSS (Basic Service Set, Conjunto de Servicios Básicos) dentro de una zona. En las redes de BSS de infraestructura, el BSSID es la dirección MAC (MediumAccess Control, Control de Acceso Medio) del AP (Access Point, Punto de acceso), y en las redes de BSS independiente o ad hoc, el BSSID se genera aleatoriamente.
Country	Un menú desplegable que permite realizar configuraciones a nivel mundial o de un determinado país. Regulaciones locales de limitación del intervalo de canales: US= en todo el mundo, Japón=1-14, Jordania= 10-13, Israel= 1-13
Max Clients	Máximo número de clientes que pueden acceder al router.
Wireless - Guest / Virtual Access Points	Este router soporta múltiples SSIDs llamados Guest SSIDs o Virtual Access Points (puntos de acceso virtuales). Para activar uno o más Guest SSIDs seleccione la casilla ☑ en la columna **Enabled**. Para ocultar un Guest SSID seleccione su casilla ☑ en la columna **Hidden**. Haga lo mismo para **Isolate Clients** y **Disable WMM Advertise.** Para una descripción más detallada de estas funciones vea en los anteriores apartados “Clients Isolation” y “Disable WMM Advertise”. Igualmente, para **Enable WMF**, **Max Clients** y **BSSID**, consulte los apartados correspondientes de esta tabla. **NOTA:** Los host inalámbricos remotos no pueden buscar Guest SSIDs.

6.2 Security (Seguridad)

La pantalla siguiente se muestra cuando está seleccionado Wireless Security. Las opciones mostradas aquí le permiten configurar las características de seguridad de la interfaz LAN inalámbrica.



Haga clic sobre **Apply / Save** para guardar los cambios en la nueva configuración.

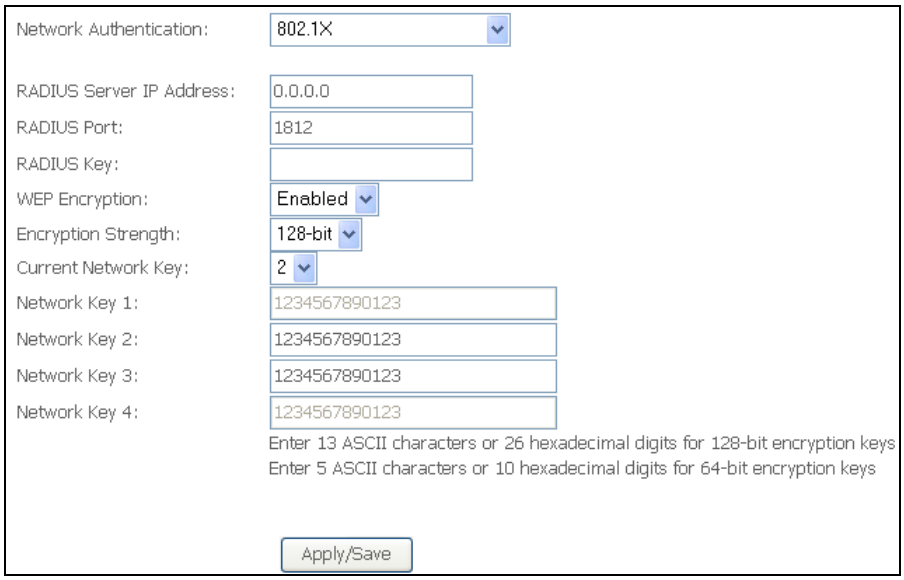
WIRELESS SECURITY (SEGURIDAD INALÁMBRICA)

Los parámetros de la seguridad inalámbrica pueden ser configurados según el Wi-Fi Protected Setup (WPS) o según el Manual Setup (Manual de instalación).El método WPS configura los parámetros de seguridad automáticamente (véase 6.2.1 WPS) mientras que el método del Manual Setup requiere que el usuario configure estos parámetros usando la Interfaz Web de usuario (véase la tabla inferior).

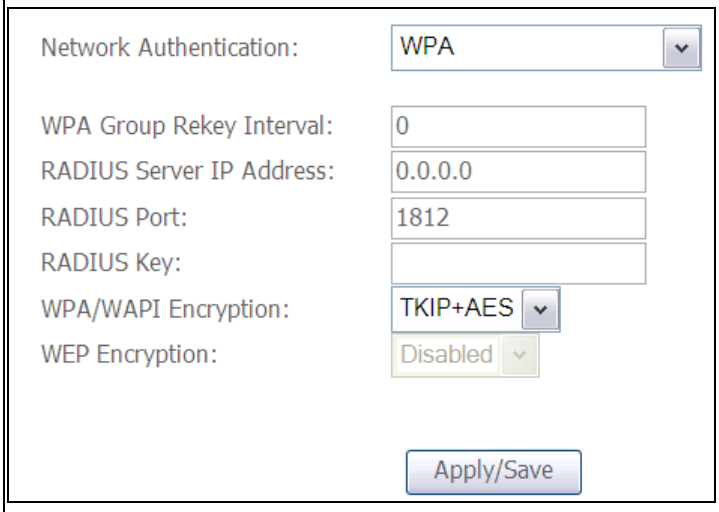
Select SSID (Seleccionar SSID)
Seleccione el nombre de red inalámbrica en la lista desplegable. SSID corresponde a Service Set Identifier (Identificador de conjunto de servicios). Todas las estaciones deben estar configuradas con el SSID correcto para acceder a la WLAN. Si el SSID no corresponde con el de la WLAN, no se permitirá el acceso al cliente.

Network Authentication (Autentificación de red)
Esta opción especifica si se utiliza una clave de red para la autentificación de la red inalámbrica. Si la autentificación de la red está establecida como Open, entonces no se proporciona autentificación. A pesar de lo cual, se seguirá verificando la identidad del cliente.

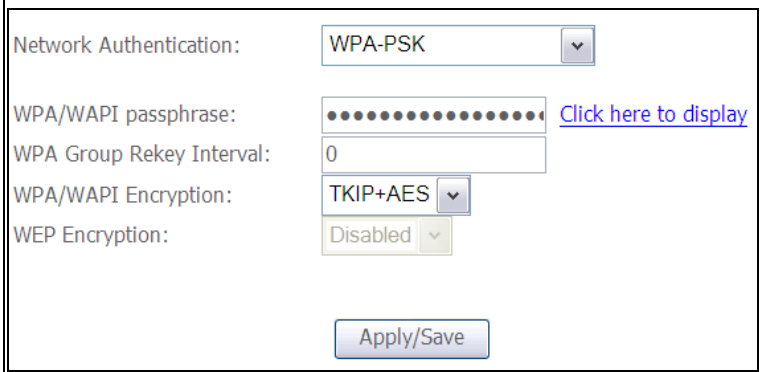
Cada tipo de autentificación posee sus propios ajustes. Por ejemplo, seleccionando autentificación 802.1X se revelará la dirección IP del servidor RADIUS, el Puerto y los campos clave. El Cifrado WEP se activará como se muestra más abajo.


Network Authentication: 802.1X
RADIUS Server IP Address: 0.0.0.0
RADIUS Port: 1812
RADIUS Key:
WEP Encryption: Enabled
Encryption Strength: 128-bit
Current Network Key: 2
Network Key 1: 1234567890123
Network Key 2: 1234567890123
Network Key 3: 1234567890123
Network Key 4: 1234567890123
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys
Apply/Save

La configuración para la autentificación WPA se muestra debajo.



A continuación se muestra la configuración de la autentificación WPA-PSK.



WEP Encryption (Cifrado WEP)
Esta opción especifica si los datos que se transmiten por la red están encriptados. La misma clave de red es utilizada para el cifrado y la autentificación de la red. Pueden definirse cuatro claves de red aunque no es posible usar más de una a la vez. Utilice la lista Current Network Key para seleccionar la clave de red apropiada. Las opciones de seguridad incluyen servicios de autentificación y cifrado basados en el algoritmo Wired Equivalent Privacy (WEP). WEP es un conjunto de servicios de seguridad usados para proteger las redes 802.11 de accesos no autorizados, como en este caso la captura del tráfico de la red inalámbrica. Cuando el cifrado o encriptación de datos está activo, se generan unas claves de encriptación secretas que son utilizadas por la estación de origen y la de destino para alterar los bits de la trama. En el modo de autentificación de claves compartida, cada estación inalámbrica asume que ha recibido una clave compartida secreta a través de un canal seguro que es independiente del canal de comunicaciones de la red inalámbrica 802.11.
Encryption Strength (Fiabilidad de la clave)
Esta lista desplegable se muestra cuando el Cifrado WEP está activo. La fiabilidad de la clave es proporcional al número de bits binario que constituye la clave. Esto quiere decir que las claves con un mayor número de bits poseen un mayor nivel de seguridad y son más difíciles de descifrar. La fiabilidad del cifrado puede establecerse en 64-bit o 128-bit. Una clave de 64-bit es el equivalente a 5 caracteres ASCII o 10 números hexadecimales. Una clave de 128-bit contiene 13 caracteres ASCII o 26 números hexadecimales. Cada clave contiene un encabezado de 24-bit (un vector de inicio) que permite la decodificación paralela de múltiples flujos de datos encriptados.

6.2.1 WPS

Wi-Fi Protected Setup (WPS) es un estándar de industria que simplifica la configuración de la seguridad inalámbrica para dispositivos de red certificados. Cada dispositivo certificado según el estándar WPS tiene un número PIN y un botón, localizado en el dispositivo o accesible a través del software del dispositivo. El AR-5387un tiene ambos, un botón WPS en el dispositivo y un botón virtual accesible desde la interfaz Web de usuario (WUI).

Los dispositivos que soportan el estándar WPS portan el logo de WPS (mostrado aquí). Aunque el logo de WPS no aparezca en su dispositivo, éste podría, sin embargo, soportar WPS, para cercionarse, verifíquelo en la documentación del dispositivo en el apartado "Wi-Fi Protected Setup".

NOTA:	WPS está únicamente disponible en los modos de autentificación de red Open, WPA-PSK, WPA2-PSK y Mixed WPA2/WPA-PSK . Otros modos de autentificación no usan WPS, por lo que se debe configurar de forma manual.

Para configurar los parámetros de seguridad con WPS, siga el procedimiento indicado más abajo. Debe elegir entre el método de configuración por PIN o por Botón Pulsador (Push-Button) para los pasos 6 y 7.

I. Setup (Instalación)

PASO 1: Active WPS seleccionando **Enabled** en la lista desplegable mostrada a continuación.

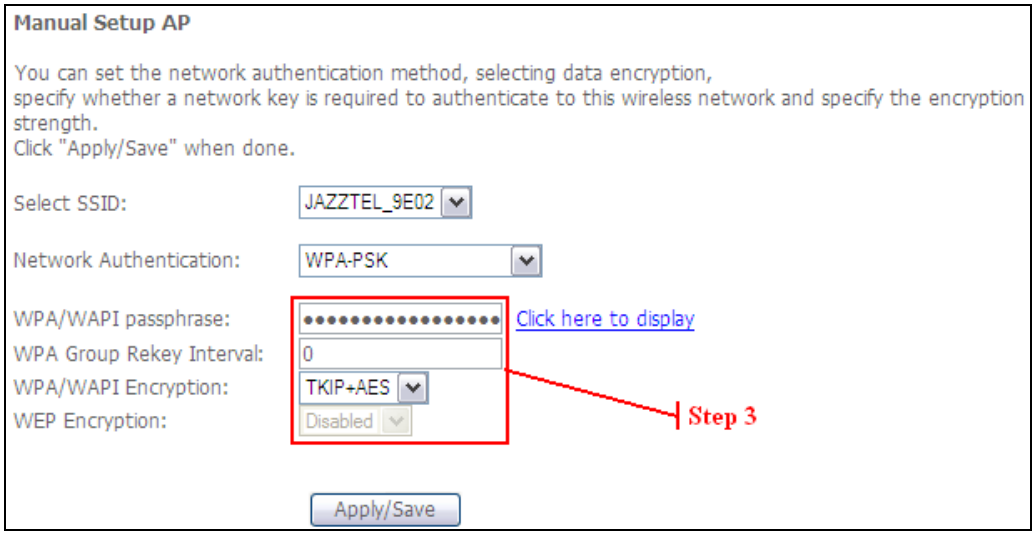
PASO 2: Establezca el WPS AP Mode. Se usa **Configured** cuando el AR-5387un va a asignar configuraciones de seguridad a los clientes. Se usa **Unconfigured** cuando un cliente externo asigna configuraciones de seguridad al AR-5387un.

NOTAS: Su cliente puede tener o no la capacidad de proporcionar configuraciones de seguridad al AR-5387un. Si no la tiene, usted debe establecer en el WPS AP Mode el modo Configured. Consulte la documentación del dispositivo para verificar sus posibilidades.

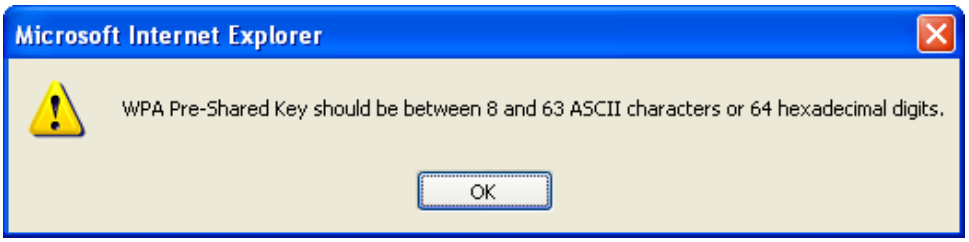
Por otro lado, si usa Windows Vista, puede añadir un registro externo usando el botón **StartAddER** (en Apéndice E – Funcionamiento WPS tiene instrucciones detalladas).

II. Network Authentication (Autentificación de red)

PASO 3: Seleccione el modo de autentificación de red Open, WPA-PSK, WPA2-PSK, o Mixed WPA2/WPA-PSK en la sección Manual Setup AP de la pantalla Wireless Security. El ejemplo de abajo muestra el modo WPA2-PSK.



PASO 4: Para el modo Pre-Shared Key (PSK), introduzca una clave pre-compartida WPA (Pre-Shared Key de WPA). Aparecerá el siguiente cuadro de diálogo en caso de que la Key (clave) sea demasiado corta o demasiado larga.



PASO 5: Haga clic en el botón **Save / Apply** en la parte inferior de la pantalla.

III a. PUSH-BUTTON CONFIGURATION (CONFIGURACIÓN CON BOTÓN PULSADOR)

La configuración WPS con botón pulsador es un método de configuración semi-automático. Puede usarse el botón WPS situado en el panel posterior del router o también mediante la Interfaz Web de usuario (WUI).

El proceso de configuración WPS con botón pulsador se describe más abajo. Se da por supuesto que la función Wireless está Activada y el router está configurado como el punto de acceso (PA) inalámbrico de su WLAN. Además, el cliente con conexión inalámbrica debe estar configurado correctamente y estar en funcionamiento con la función WPS activada.

NOTA:	El punto de acceso inalámbrico del router realiza la acción de búsqueda durante 2 minutos. Si el router detiene la búsqueda antes de que usted haya completado el Paso 7, vuelva al Paso 6.

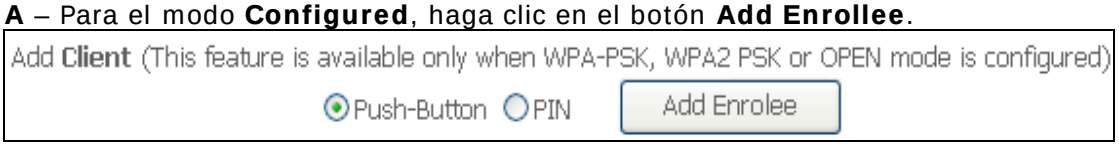
PASO 6: **Primer método: Botón WPS**

Presione el botón WPS situado en el panel posterior del router. El LED WPS brillará intermitentemente indicando que el router ha comenzado a buscar un cliente.

Segundo método: Botón virtual del WUI

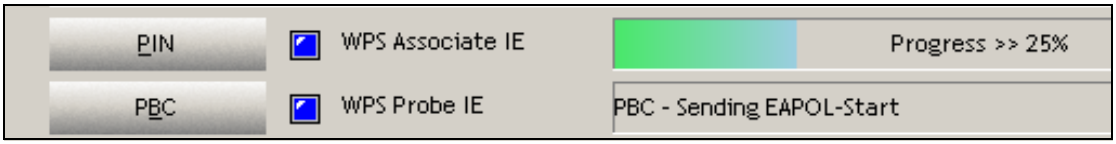
Seleccione la opción Push-Button en la sección WSC Setup de la pantalla Wireless Security, como se muestra en **A** o en **B** más abajo, y a continuación haga clic en el botón correspondiente en función del WSC AP Mode seleccionado en el Paso 2.

A – Para el modo **Configured**, haga clic en el botón **Add Enrollee**.



B – Para el modo **Unconfigured**, haga clic en el botón **Config AP**.

PASO 7: Vaya a su cliente inalámbrico WPS y active la función push-button. Debajo se muestra, a modo de ejemplo, la pantalla de un cliente WPS tipo.



Ahora vaya al Paso 8 (parte IV. Check Connection) para comprobar la conexión WPS.

IIIb. WPS – PIN CONFIGURATION (CONFIGURACIÓN PIN)

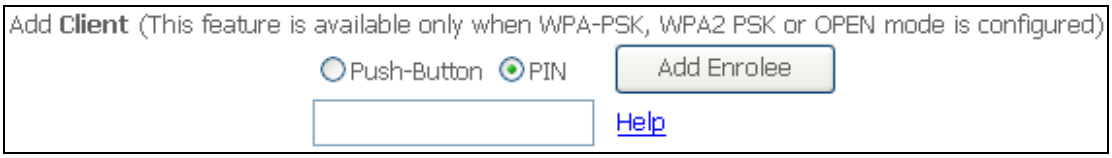
Mediante este método, los parámetros de seguridad se configuran a través de un número de identificación personal (PIN). El PIN se puede encontrar en el dispositivo mismo o en el software. Así mismo, el PIN se puede generar posteriormente de forma aleatoria. Para obtener su número PIN de cliente, compruebe en la documentación del dispositivo las instrucciones específicas al respecto.

El proceso de configuración WPS mediante PIN se describe más abajo. Se da por supuesto que la función Wireless está Activada y el router está configurado como el punto de acceso (PA) inalámbrico de su LAN. Además, el cliente con conexión inalámbrica debe estar configurado correctamente y estar en funcionamiento con la función WPS activada.

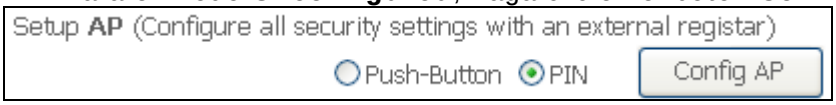
NOTA:	Al contrario que el método Push-button, el método PIN no tiene establecido un tiempo de ajuste. Lo cual quiere decir que el router seguirá buscando hasta que encuentre un cliente.

PASO 6: Seleccione la opción PIN en la sección WSC Setup de la pantalla Wireless Security, como se muestra en **A** o en **B** más abajo, y a continuación haga clic en el botón correspondiente en función del WSC AP Mode seleccionado en el Paso 2.

A – Para el modo **Configured**, introduzca el PIN del cliente en el campo provisto a tal efecto y haga clic a continuación en el botón **Add Enrollee** (Véase debajo).

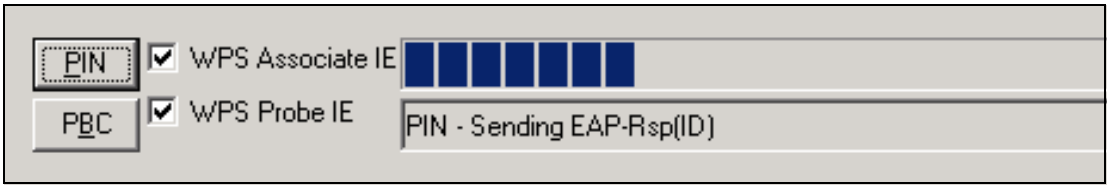

Add Client (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)
Push-Button
PIN
Add Enrolee
Help

B – Para el modo **Unconfigured**, haga clic en el botón **Config AP**.



PASO 7: Active la función PIN en el cliente inalámbrico. Para el modo **Configured**, el cliente se debe configurar como Enrollee. Para el modo **Unconfigured**, el cliente se debe configurar como Registrar. Esta función no tiene nada que ver con la función External Registrar de Windows Vista.

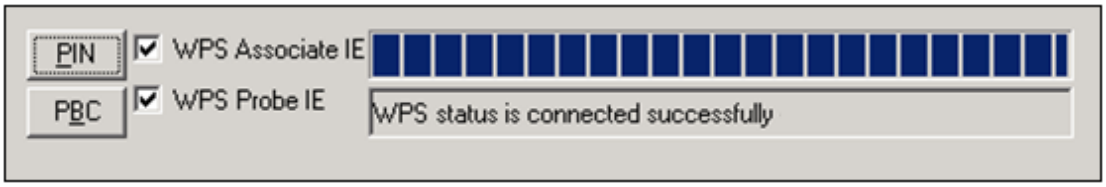
La imagen nos proporciona un ejemplo de la función PIN de un cliente WPS en progreso.



Ahora vaya al Paso 8 (parte IV. Check Connection) para comprobar la conexión WPS.

IV. CHECK CONNECTION (VERIFICACIÓN DE LA CONEXIÓN)

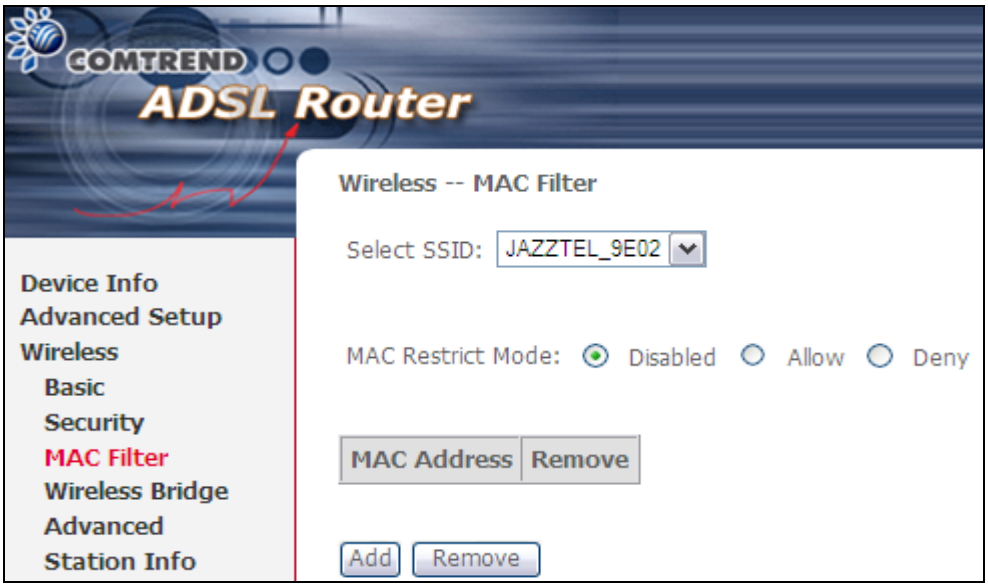
PASO 8: Si el método de configuración WPS ha tenido éxito, usted será capaz de acceder al PA inalámbrico desde el cliente. El estado de la conexión aparecerá en el software del cliente. En el ejemplo de abajo se muestra que la conexión se ha establecido correctamente.



Puede hacer doble clic en el icono Wireless Network Connection (Conexión de red inalámbrica) desde la ventana Network Connections (o el sistema tray) para confirmar el estado de la nueva conexión.

6.3 MAC Filter (Filtro MAC)

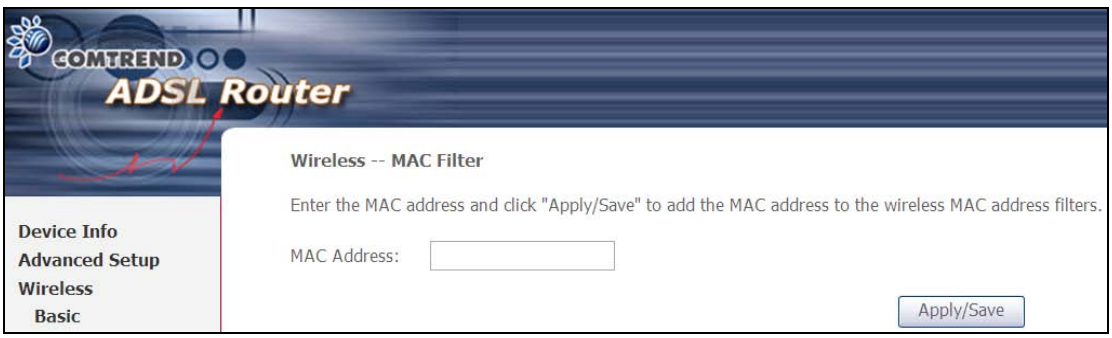
Esta opción permite restringir el acceso al router en función de la dirección MAC. Para añadir un filtro de direcciones MAC haga clic sobre el botón **Add**, como se muestra debajo. Para eliminar un filtro, selecciónelo en la tabla de direcciones MAC y haga clic en el botón **Remove**.



Opción	Descripción
Select SSID	Seleccione el nombre de red inalámbrica en la lista desplegable. SSID corresponde a Service Set Identifier (Identificador de conjunto de servicios). Todas las estaciones deben estar configuradas con el SSID correcto para acceder a la WLAN. Si el SSID no corresponde con el de la WLAN, el usuario no podrá tener acceso.
MAC Restrict Mode	Disabled: El filtro MAC esta desactivado. Allow: Permite el acceso a las direcciones MAC especificadas. Deny: Deniega el acceso a las direcciones MAC especificadas.
MAC Address	Muestra un listado de las direcciones MAC sujetas al modo MAC Restrict Mode. Se pueden añadir un máximo de 60 direcciones MAC. Cada dispositivo de red posee una dirección MAC de 48 bits única. Normalmente esta dirección se muestra como xx.xx.xx.xx.xx.xx, donde xx son número hexadecimales.

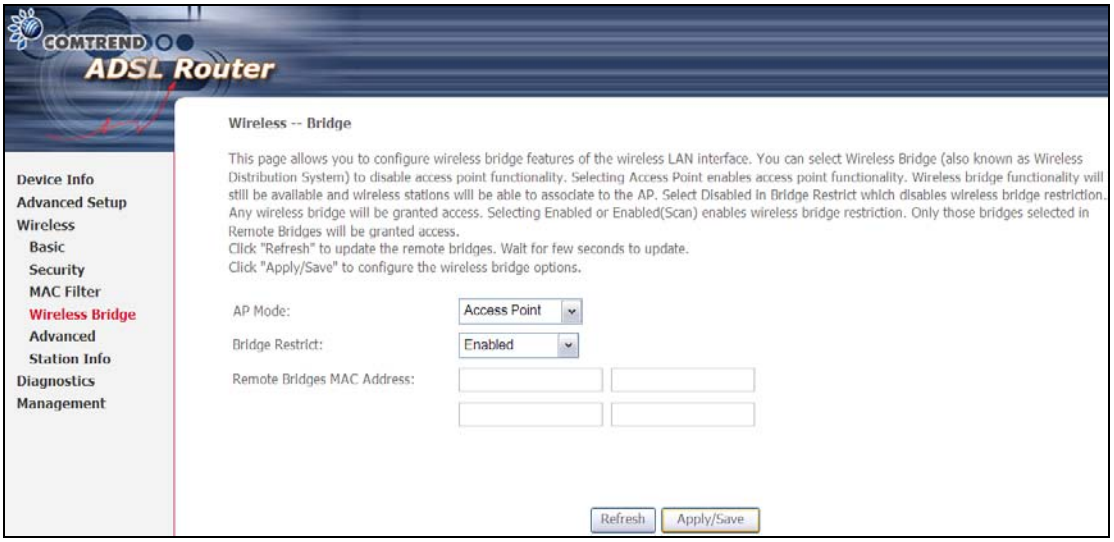
Tras hacer clic sobre **Add** se mostrará la siguiente pantalla.

Introduzca la dirección MAC en el campo suministrado y haga clic sobre **Save / Apply**.



6.4 Wireless Bridge (Puente inalámbrico)

Esta pantalla permite la configuración de las características del Puente inalámbrico de la interfaz WAN. Véase la tabla inferior para conocer más detalles de las distintas opciones.

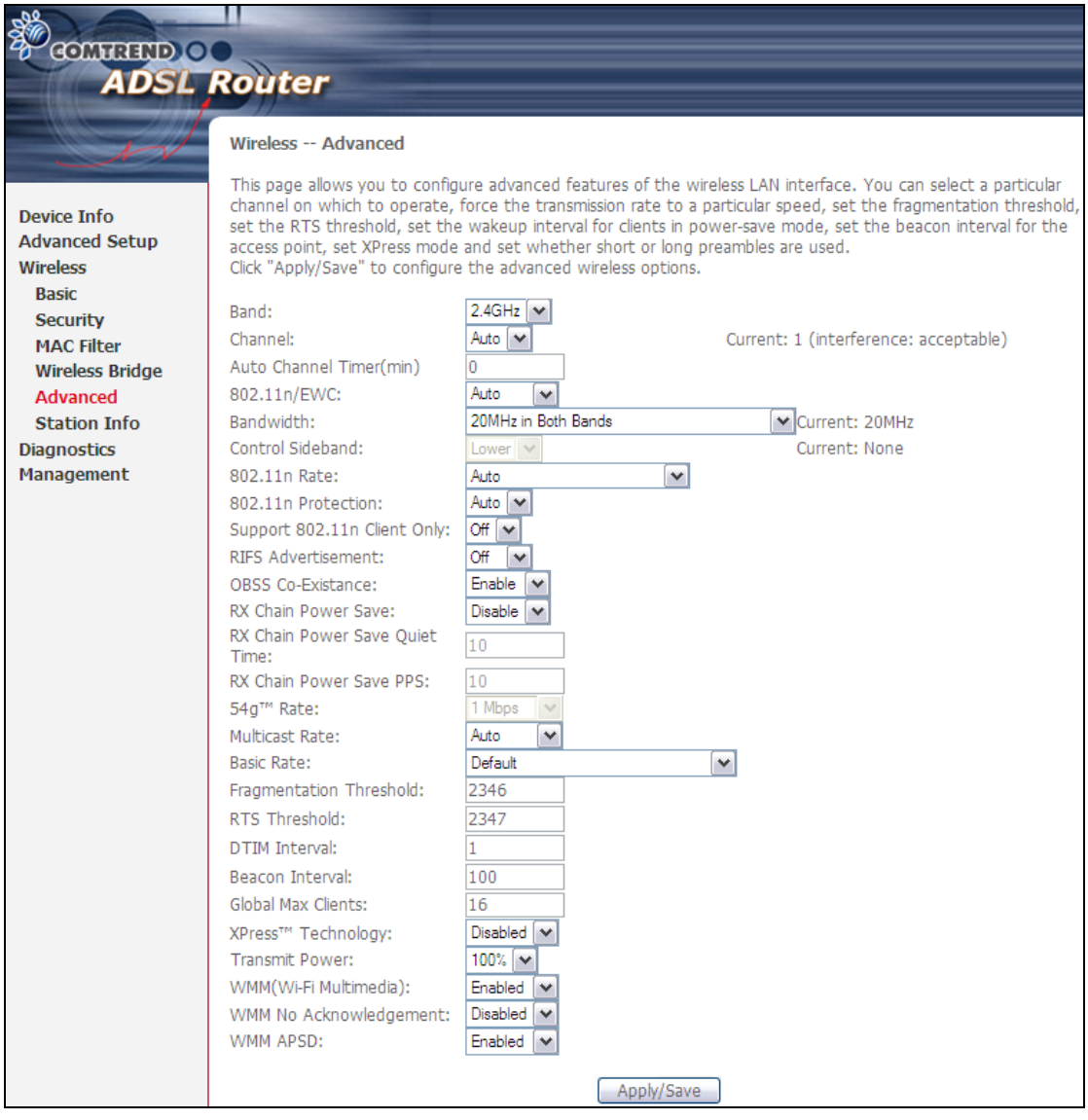

COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management
Wireless -- Bridge
This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.
AP Mode:
Access Point
Bridge Restrict:
Enabled
Remote Bridges MAC Address:
Refresh
Apply/Save

Haga clic sobre **Apply / Save** para guardar los cambios en la nueva configuración.

Característica	Descripción
AP Mode	Seleccionando **Wireless Bridge** (también conocido como Wireless Distribution System) se desactiva la funcionalidad de Punto de Acceso (PA), mientras que al seleccionar **Access Point** se activa su funcionalidad. En el modo **Access Point**, la funcionalidad Puente inalámbrico todavía sigue disponible y las estaciones inalámbricas podrán asociarse al Punto de Acceso.
Bridge Restrict	Seleccionando **Disabled** se desactiva la restricción del Puente inalámbrico, lo que implica que se validará el acceso a cualquier puente inalámbrico. Seleccionando **Enabled** o **Enabled (Scan)** se activa la restricción de Puente inalámbrico. Solamente se les dará acceso a aquellos puentes seleccionados en la lista Remote Bridges. Haga clic sobre **Refresh** para actualizar la lista de estaciones cuando Bridge Restrict está activo.

6.5 Advanced (Función inalámbrica avanzada)

La pantalla Advanced le permite configurar las características avanzadas de la interfaz LAN inalámbrica. Se puede seleccionar un determinado canal en el que operar, fijar la velocidad de transmisión en un determinado valor, establecer el umbral de fragmentación, fijar el umbral RTS, establecer el intervalo de activación para los clientes que se encuentren en modo de ahorro de energía, establecer el intervalo de baliza para el punto de acceso, establecer el modo XPress y configurar la utilización de preámbulos cortos o largos. Haga clic sobre **Apply/Save** para establecer las nuevas funciones inalámbricas avanzadas.


COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management
Wireless -- Advanced
This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.
Click "Apply/Save" to configure the advanced wireless options.
Band: 2.4GHz
Channel: Auto Current: 1 (interference: acceptable)
Auto Channel Timer(min) 0
802.11n/EWC: Auto
Bandwidth: 20MHz in Both Bands Current: 20MHz
Control Sideband: Lower Current: None
802.11n Rate: Auto
802.11n Protection: Auto
Support 802.11n Client Only: Off
RIFS Advertisement: Off
OBSS Co-Existance: Enable
RX Chain Power Save: Disable
RX Chain Power Save Quiet Time: 10
RX Chain Power Save PPS: 10
54g™ Rate: 1 Mbps
Multicast Rate: Auto
Basic Rate: Default
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
Global Max Clients: 16
XPress™ Technology: Disabled
Transmit Power: 100%
WMM(Wi-Fi Multimedia): Enabled
WMM No Acknowledgement: Disabled
WMM APSD: Enabled
Apply/Save

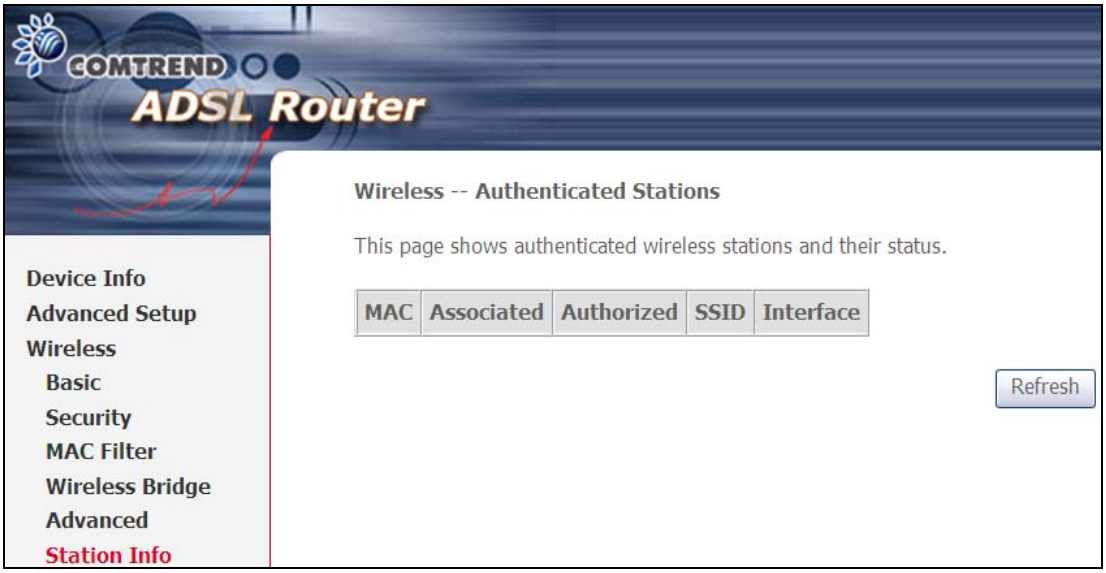
Campo	Descripción
Band	Establezca la banda de frecuencias de 2.4 GHz para garantizar la compatibilidad con los estándares IEEE 802.11x. La nueva revisión permite a las unidades IEEE 802.11n reducir la velocidad de modo que los dispositivos más antiguos IEEE 802.11x puedan coexistir en la misma red. El estándar IEEE 802.11g crea una paridad de datos a 2.4 GHz con el estándar IEEE 802.11a, que tiene una velocidad de 54 Mbps a 5GHz. (El estándar IEES 802.11a tiene otras diferencias con respecto al IEEE 802.11b o g. tales como la oferta de un mayor número de canales.)
Channel	Menú desplegable que permite la selección de un determinado canal.
Auto Channel Timer (min)	Temporizador de exploración automática de canales en minutos (0 para desactivar)
802.11n/EWC	Configuración del estándar de interoperatibilidad de equipo basado en el estándar IEEE 802.11n borrador 2.0 y Enhanced Wireless Consortium (EWC)
Bandwidth	Seleccione un ancho de banda de 20GHz ó 40GHz. El ancho de banda de 40GHz utiliza dos bandas de 20GHz adyacentes para incrementar el rendimiento.
Control Sideband	Seleccione Upper o Lower sideband cuando trabaja en modo 40GHz.
802.11n Rate	Establece la tasa de transmisión física (PHY).
802.11n Protection	Desactivar para maximizar el rendimiento. Activar para mayor seguridad.
Support 802.11n Client Only	Apagar para permitir a los clientes 802.11b/g acceder al router. Activar para prohibir a los clientes 802.11b/g acceder al router.
RIFS Advertisement	Características de uno de los n-draft designados para mejorar la eficiencia. Proporciona un retraso más pequeño entre las transmisiones OFDM que en 802.11a ó g.
OBSS Co-Existance	Coexistencia entre 20 MHZ y 40 MHZ OBSS (Overlapping Basic Service Set) en WLAN
RX Chain Power Save	Activando esta característica se apaga uno de los Receive Chains, ahorrando energía al pasar de 2x2 a 2x1.
RX Chain Power Save Quiet Time	El número de segundos que el tráfico debe estar por debajo del valor PPS antes de que la función de Ahorro de Energía del RX Chain se active por sí misma.
RX Chain Power Save PPS	El número máximo de paquetes por segundo que se pueden procesar en la interfaz WLAN para durante una Quiet Time, descrita arriba, antes de que la función de Ahorro de Energía del RX Chain se active por sí misma.

Campo	Descripción
54g Rate	Menú desplegable que especifica las siguientes velocidades fijas: Auto: Predeterminado. Utiliza una velocidad de datos de 11 Mbps cuando es posible, pero reduce la velocidad a tasas inferiores cuando es necesario. Velocidades fijas de 1 Mbps, 2Mbps, 5.5Mbps ó 11Mbps. La configuración apropiada depende de la potencia de la señal.
Multicast Rate	Se configura la velocidad de transmisión de los paquetes de multidifusión (1-54 Mbps)
Basic Rate	Se configura la velocidad de transmisión básica.
Fragmentation Threshold	Es un umbral, en bytes, que determina si los paquetes serán fragmentados y a qué tamaño. En una WLAN 802.11, los paquetes cuyo tamaño sobrepasa el umbral de fragmentación son fragmentados; es decir, divididos en unidades más pequeñas adecuadas al tamaño del circuito. Por el contrario, no se fragmentan los paquetes inferiores al valor del umbral de fragmentación. Introduzca un valor entre 256 y 2346. Si se produce una tasa elevada de error de paquetes, intente aumentar ligeramente su umbral de fragmentación. El valor debe ajustarse a la configuración predeterminada de 2346. Si se fija el umbral de fragmentación en un valor demasiado bajo el rendimiento puede ser insuficiente.
RTS Threshold	El umbral RTS (Request to Send), fijado en bytes, especifica el tamaño de paquete por encima del cual la tarjeta WLAN recurre al mecanismo RTS/CTS. Los paquetes que superan el umbral RTS especificado activan el mecanismo RTS/CTS. La tarjeta NIC transmite paquetes de menor tamaño sin recurrir al mecanismo RTS/CTS. El valor predeterminado de 2347 (longitud máxima) desactiva el umbral RTS.
DTIM Interval	DTIM (Delivery Traffic Indication Message), conocido también como intervalo de baliza. El valor del intervalo de entrada está entre 1 y 65535. El intervalo DTIM es una cuenta atrás que avisa a los clientes de la siguiente ventana para que estén pendientes de los mensajes de emisión y multidifusión. Cuando un punto de acceso ha emitido dichos mensajes para clientes asociados, envía el siguiente DTIM con un valor de intervalo DTIM. Los clientes del punto de acceso oyen la baliza y se preparan para recibir los mensajes de emisión y multidifusión. El valor predeterminado es 1.

Campo	Descripción
Beacon Interval	Es el tiempo transcurrido entre las transmisiones de balizas medido en milisegundos. Por defecto es 100 ms. y el rango aceptable es 1 - 65535. Cada transmisión de baliza identifica la presencia de un punto de acceso. Por defecto, los dispositivos de red rastrean de forma pasiva todos los canales RF y están pendientes de las balizas procedentes de puntos de acceso con el fin de encontrar un punto de acceso adecuado. Antes de que una estación entre en el modo de ahorro de energía, necesita que el intervalo de baliza sepa cuándo debe activarse para recibir la baliza (y saber si existen tramas de búfer en el punto de acceso).
Global Max Clients	Máximo número de clientes que pueden conectarse al router.
Xpress ™ Technology	La tecnología Xpress se ajusta a la proposiciones de especificación de los dos estándares industriales planeados en materia de dispositivos inalámbricos.
Transmit Power	Establece la potencia de salida (en porcentaje) como se desee.
WMM (Wi-Fi Multimedia)	La tecnología mantiene la prioridad para las aplicaciones de audio, vídeo y voz en una red Wi-Fi. Permite que el servicio multimedia posea una mayor prioridad.
WMM No Acknowledgement	Se refiere al reconocimiento de la política usada a nivel MAC. Activando No Acknowledgement puede lograrse un mayor rendimiento pero mayor tasa de errores en un entorno con un nivel de ruido de radio frecuencia (RF) elevada.
WMM APSD	Esto es el Automatic Power Save Delivery. Ahorra energía.

6.6 Station Info (Información de la estación)

Esta página muestra las estaciones inalámbricas autentificadas y su estado. Haga clic en el botón **Refresh** para actualizar la lista de estaciones en la WLAN.

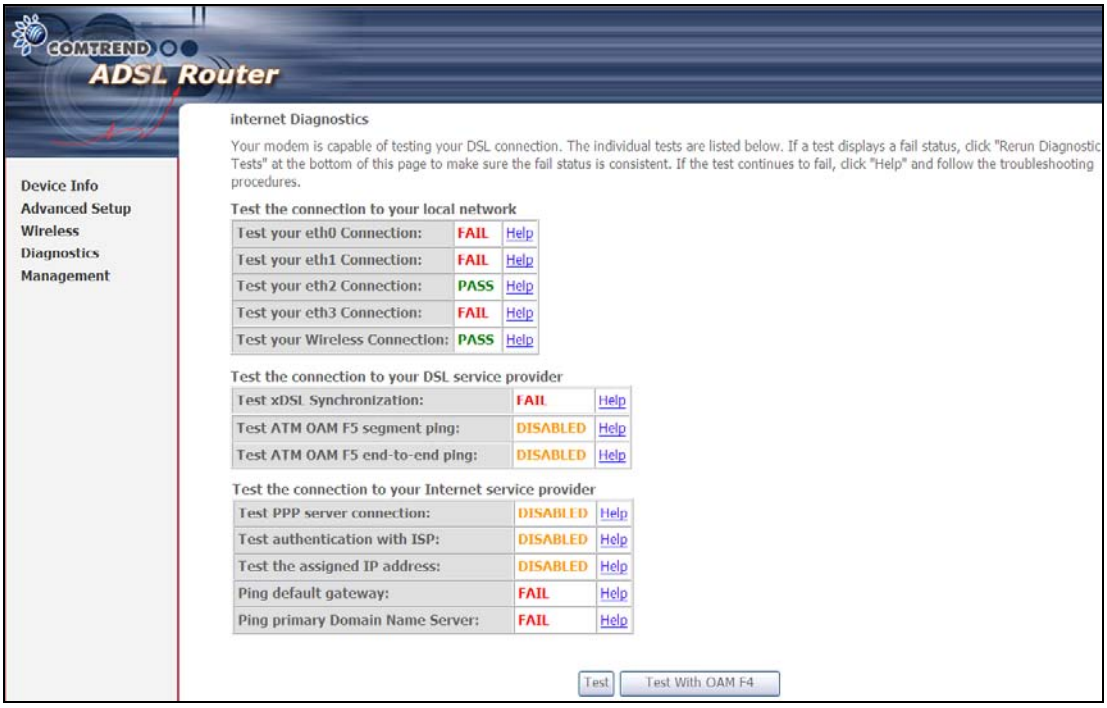


Consulte la tabla inferior para conocer las descripciones de las distintas opciones de la columna Encabezado.

Encabezado	Descripción
MAC	Muestra un listado con la dirección MAC de todas las estaciones.
Associated	Presenta una lista de todas las estaciones que están asociadas con un punto de acceso junto con la cantidad de tiempo desde que los paquetes fueron transferidos a/o desde cada estación. Si una estación permanece inactiva durante demasiado tiempo, es eliminada de la lista.
Authorized	Presenta una lista con los dispositivos que tienen un acceso autorizado.
SSID	Muestra cuál es el SSID del MODEM al que se conectan las estaciones.
Interface	Muestra la interfaz del módem a la que se conectan las estaciones.

Capítulo 7 Diagnósticos

La primera pantalla Diagnostics es un tablero de mandos que muestra el estado general de la conexión.
Si una de las pruebas muestra un error de estado, haga clic sobre el botón Rerun Diagnostic Tests y confirme el error.
Si la prueba continúa dando un error, haga clic en Help y siga el procedimiento de solución de problemas.


COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Diagnostics
Management
internet Diagnostics
Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Test the connection to your local network
Test your eth0 Connection: FAIL Help
Test your eth1 Connection: FAIL Help
Test your eth2 Connection: PASS Help
Test your eth3 Connection: FAIL Help
Test your Wireless Connection: PASS Help
Test the connection to your DSL service provider
Test xDSL Synchronization: FAIL Help
Test ATM OAM F5 segment ping: DISABLED Help
Test ATM OAM F5 end-to-end ping: DISABLED Help
Test the connection to your Internet service provider
Test PPP server connection: DISABLED Help
Test authentication with ISP: DISABLED Help
Test the assigned IP address: DISABLED Help
Ping default gateway: FAIL Help
Ping primary Domain Name Server: FAIL Help
Test
Test With OAM F4

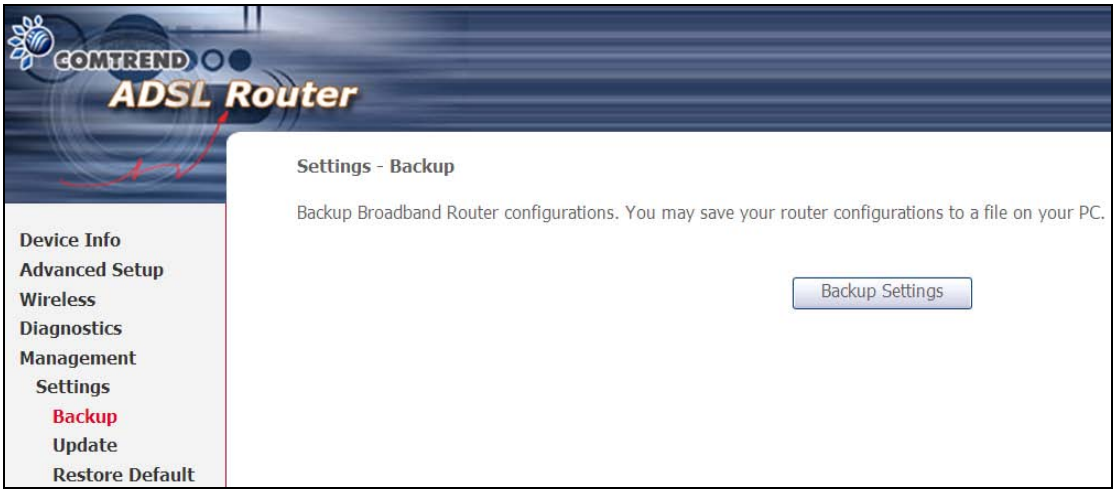
Capítulo 8 Administración

8.1 Settings (Configuración)

Este menú incluye las pantallas 8.1.1 Backup Settings (Copia de seguridad de la Configuración), 8.1.2 Update Settings (Restablecimiento de la configuración guardada), 8.1.3 Restore Default (Restablecimiento de la configuración predeterminada).

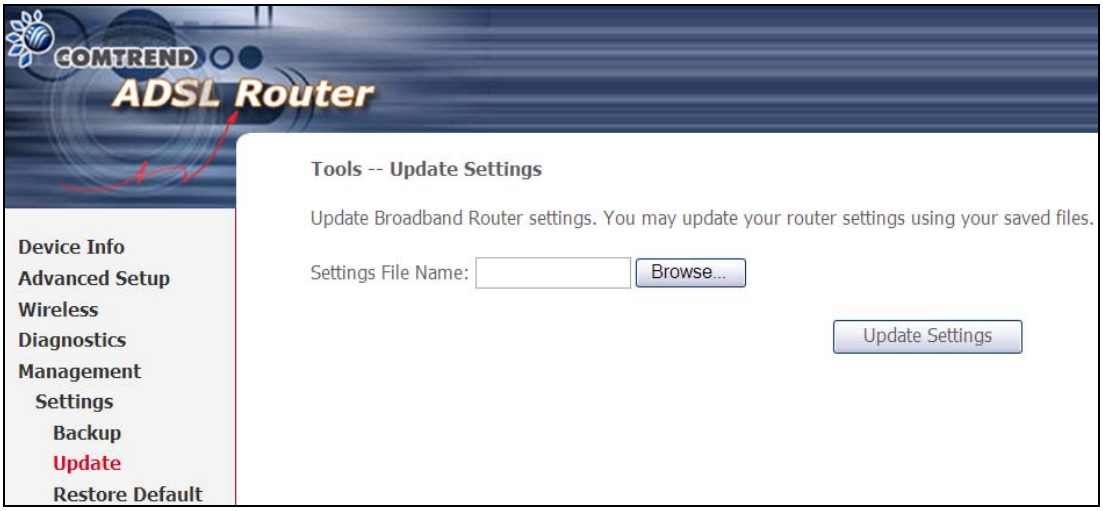
8.1.1 Backup Settings (Copia de seguridad de la Configuración)

Para guardar la configuración actual en un archivo en su PC haga clic en **Backup Settings**. Se le preguntará por una ubicación para la copia del archivo. Este archivo puede usarse posteriormente para restaurar la configuración desde la pantalla **Update Settings,** como se describe más abajo.



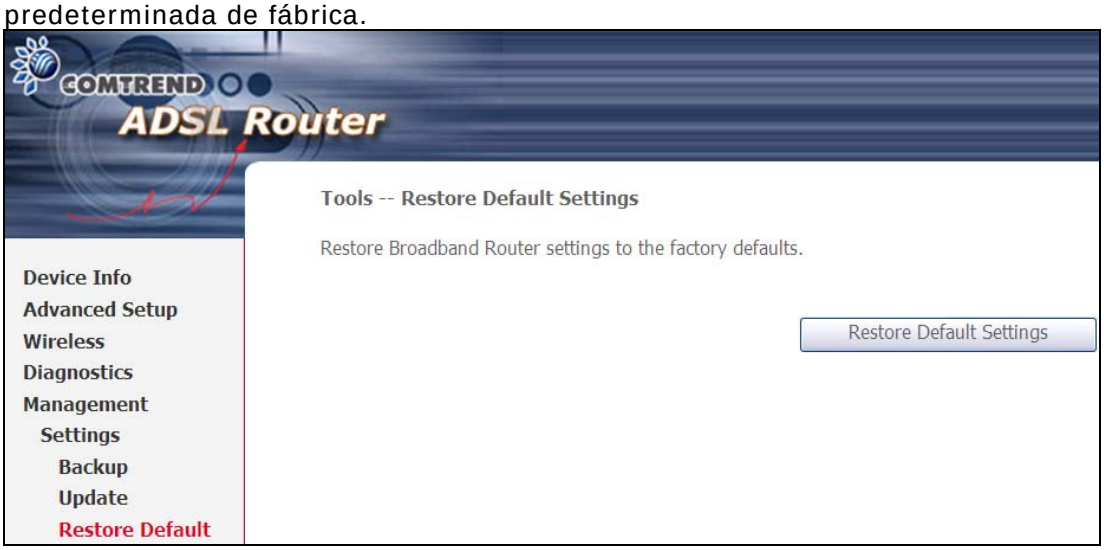
8.1.2 Update Settings (Restablecimiento de la configuración guardada)

Esta opción recupera los archivos de configuración previamente guardados mediante **Backup Settings.** Introduzca el nombre del archivo incluyendo la ruta completa en el campo **Settings File Name**, o pulse sobre **Browse...** para buscar el archivo, luego haga clic en **Update Settings** para restaurar la configuración**.**

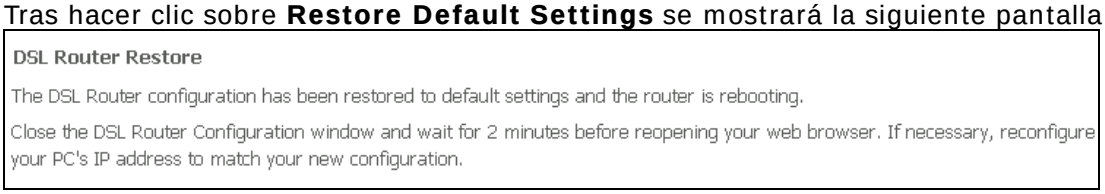


8.1.3 Restore Default (Restablecimiento de la configuración predeterminada)

Haga clic sobre **Restore Default Settings** para restaurar la configuración predeterminada de fábrica.



Tras hacer clic sobre **Restore Default Settings** se mostrará la siguiente pantalla.


DSL Router Restore
The DSL Router configuration has been restored to default settings and the router is rebooting.
Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Cierre el navegador y espere 2 minutos antes de volver a abrirlo. También puede ser necesario que tenga que reconfigurar la IP de su PC para que se ajuste a los nuevos ajustes.

NOTA:	Esta opción tiene el mismo efecto que pulsar el botón Reset del dispositivo. Tanto el hardware del AR-5387un como el programa de arranque soportan el botón Reset por defecto. Si se mantiene pulsado el botón **Reset** durante más de 5 segundos, el programa de arranque borrará los datos de configuración guardados en la memoria flash.

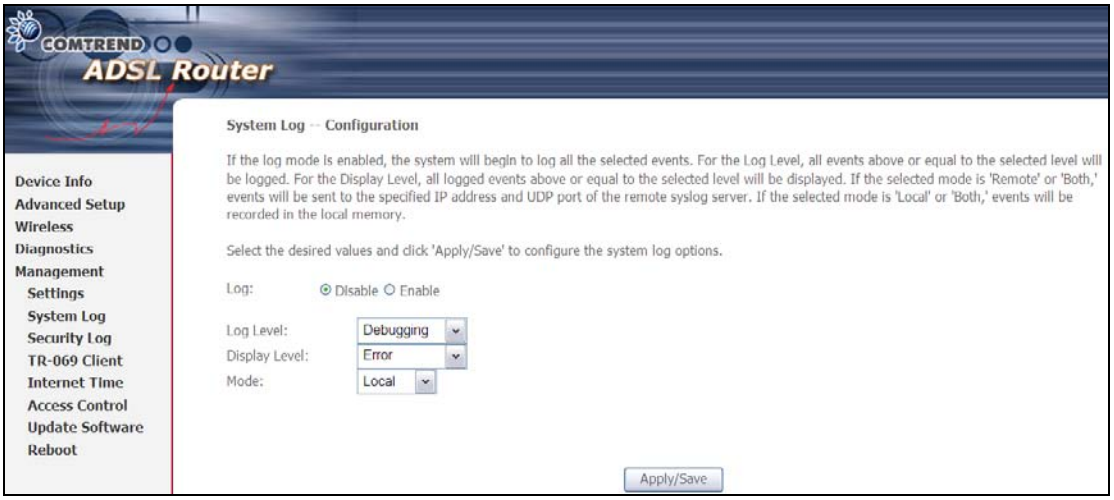
8.2 System Log (Registro del sistema)

Esta función permite crear un archivo de registro del sistema que puede guardarse y consultarse bajo petición.

Siga los siguientes pasos para continuar, activar y ver el registro del sistema.

PASO 1: Haga clic en **Configure System Log**, como se muestra debajo (resaltado en rojo)

PASO 2: Seleccione las opciones y haga clic en **Apply/Save.**

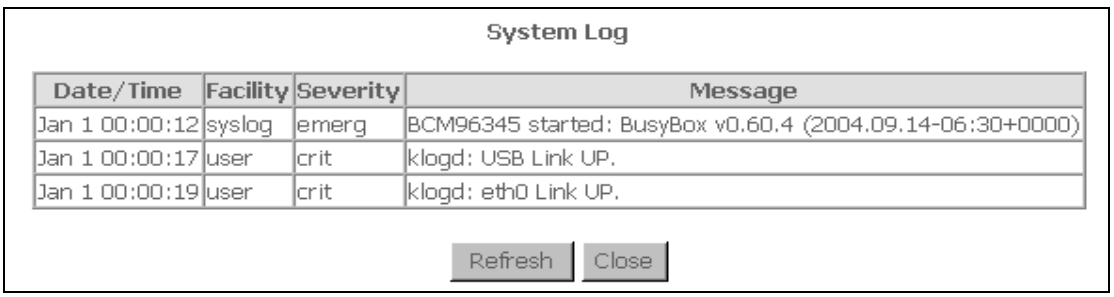

COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
Security Log
TR-069 Client
Internet Time
Access Control
Update Software
Reboot
System Log -- Configuration
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.
Select the desired values and click 'Apply/Save' to configure the system log options.
Log: Disable Enable
Log Level: Debugging
Display Level: Error
Mode: Local
Apply/Save

Consulte la tabla inferior para conocer las descripciones de las distintas opciones de registro del sistema.

Opción	Descripción
Log	Indica si el sistema está registrando las incidencias actualmente. El usuario puede activar o desactivar el registro de incidencias. Esta opción está desactivada por defecto. Para activarla, marque la casilla **Enable** y luego haga clic en **Apply/Save**.

Opción	Descripción
Log Level	Le permite configurar el nivel de la incidencia y filtrar las no deseadas por debajo de ese nivel. Las incidencias que vayan desde el nivel más grave “Emergency” hasta el nivel configurado serán guardadas en el búfer de registro de la SDRAM del AR-5387un. Cuando se llene el búfer de registro, las nuevas incidencias se colocarán en la parte superior del búfer sobrescribiendo los anteriores. Por defecto el nivel de registro es “Debugging”, que corresponde al nivel de menor gravedad. Los niveles de registro son los siguientes: · Emergency = el sistema no se puede usar · Alert = debe efectuarse una acción de inmediato · Critical = la situación es crítica · Error = se han producido errores · Warning = situación importante pero normal · Notice = normal, pero con situación no significativa · Informational = proporciona información de referencia · Debugging = mensajes a nivel de depuración Emergency es el nivel de gravedad más alto, mientras que Debugging es el menos importante. Por ejemplo, si el nivel de registro se establece en Debugging, todas las incidencias ocurridas desde el nivel más bajo “Debugging” al nivel más alto “Emergency” serán registradas. Si el nivel de registro se establece en Error, solamente se registrará “Error" y el nivel superior.
Display Level	Permite al usuario seleccionar los eventos o incidencias registradas y mostrarlas en la ventana **View System Log** para las incidencias de este nivel y superiores hasta Emergency.
Mode	Permite especificar si las incidencias deben almacenarse en la memoria local, enviarse al sistema de registro de un servidor Syslog o ambas situaciones simultáneamente. Si se selecciona el modo Remote, el sistema de visualización del registro de incidencias no será capaz de mostrar las incidencias guardadas en el servidor remoto Syslog. Cuando se selecciona el modo Remote o Both, la interfaz Web de usuario pedirá al usuario que introduzca la dirección IP y el puerto UDP del servidor.

PASO 3: Haga clic en **View System Log**. Los resultados se mostrarán de la siguiente forma.



8.3 Security Log (Registro de seguridad)

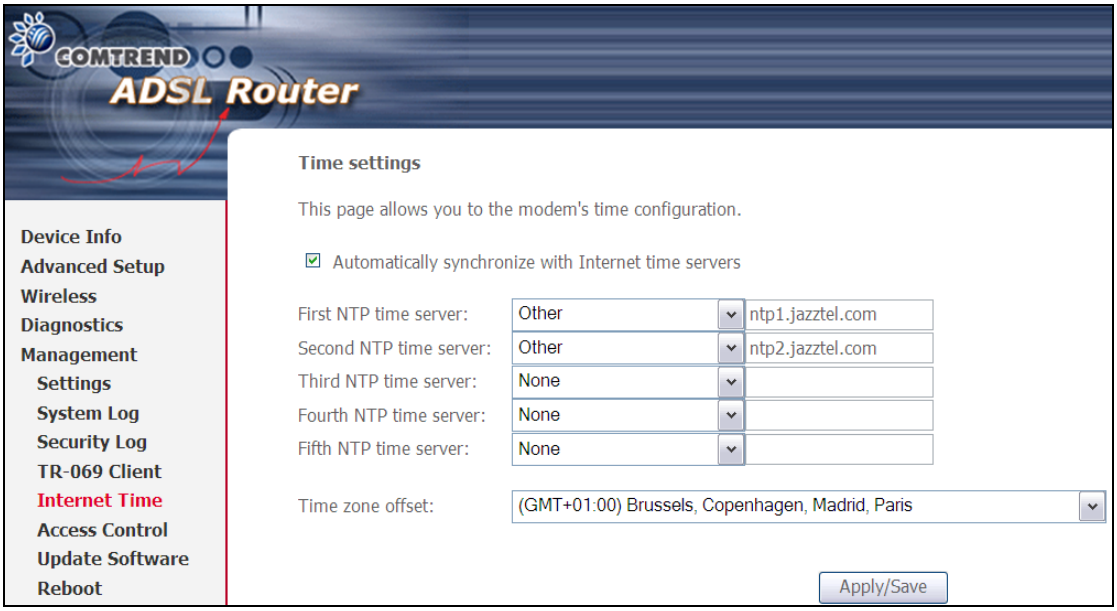
El cuadro de diálogo del registro de seguridad le permite ver el registro de seguridad y configurar las opciones del registro de seguridad.

Haga clic en “View” para ver el registro de seguridad.

Haga clic en “Reset” para eliminar y reiniciar el registro de seguridad.

8.4 Internet Time (Hora de Internet)

Esta opción sincroniza automáticamente la hora del router con la de los Internet timeservers. Para activar la sincronización de hora, marque la casilla correspondiente ☑, escoja su servidor de hora preferido, seleccione la zona horaria correcta y haga clic en **Save / Apply.**



NOTA:	Este menú no se muestra en el modo Bridge, ya que en este caso el router no puede conectarse al NTP timeserver.

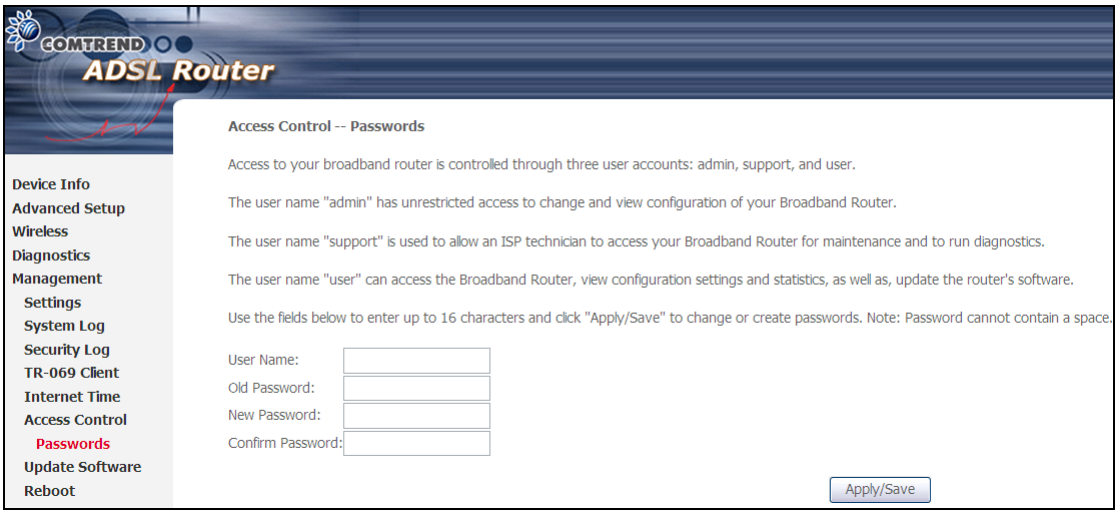
8.5 Access Control (Control de acceso)

8.5.1 Password (Contraseñas)

Esta pantalla se utiliza para configurar las contraseñas de acceso a las cuentas de usuario del dispositivo. El acceso al AR-5387un se controla a través de las tres cuentas de usuario siguientes:

- **admin** – acceso sin restricciones para cambiar o ver la configuración.
- **support** – usada para el mantenimiento remoto y los diagnósticos del router.
- **user** – puede ver los ajustes de configuración y las estadísticas y actualizar el firmware.

Utilice los campos inferiores para cambiar la configuración de contraseñas. Haga clic sobre **Save / Apply** para continuar.


COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
Security Log
TR-069 Client
Internet Time
Access Control
Passwords
Update Software
Reboot
Access Control -- Passwords
Access to your broadband router is controlled through three user accounts: admin, support, and user.
The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.
The user name "support" is used to allow an ISP technician to access your Broadband Router for maintenance and to run diagnostics.
The user name "user" can access the Broadband Router, view configuration settings and statistics, as well as, update the router's software.
Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.
User Name:
Old Password:
New Password:
Confirm Password:
Apply/Save

NOTA: Las contraseñas pueden tener una longitud de hasta 16 caracteres.

8.6 Update Software (Actualización)

Esta opción permite la actualización del firmware desde un archivo almacenado localmente.

COMTREND
ADSL Router
Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
Security Log
TR-069 Client
Internet Time
Access Control
Update Software
Reboot
Tools -- Update Software
Step 1: Obtain an updated software image file from your ISP.
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
Step 3: Click the "Update Software" button once to upload the new image file.
NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.
Software File Name:
Browse...
Update Software

PASO 1: Obtenga un archivo de imagen del software actualizado de su ISP.

PASO 2: Introduzca la ruta al archivo de imagen del firmware en el campo **Software File Name** o haga clic sobre el botón **Browse** para localizar el archivo de imagen.

PASO 3: Haga clic una vez en el botón **Update Software** para cargar el nuevo software.

NOTA: El proceso de actualización se llevará a cabo en aproximadamente 2 minutos. El dispositivo se reiniciará y la ventana del navegador actualizará la pantalla que muestra el progreso de instalación. Se recomienda que compare la **versión del Software** que aparece en la pantalla Capítulo 4 Información del dispositivo con la versión del firmware instalada, para confirmar que la instalación se ha realizado correctamente.

8.7 Reboot (Reiniciar)

Para guardar la configuración actual y reiniciar el router haga clic en **Save / Reboot.**

NOTA: Puede ser que tenga que cerrar el navegador y esperar 2 minutos antes de volver a abrirlo. También puede ser necesario que tenga que reconfigurar la IP de su PC.

Apéndice A – Firewall (Cortafuegos)

STATEFUL PACKET INSPECTION (Inspección del estado de paquetes)
Hace referencia a una arquitectura donde el cortafuegos monitoriza en cada conexión todos paquetes que atraviesan las interfaces y se asegura de que son válidos. Este método contrasta con el de filtrado de paquetes estático que solamente examina un paquete basándose en al información de su encabezado.

DENIAL OF SERVICE ATTACK (Denegación del ataque de servicio)
Es un incidente en el cual un usuario u organización es privado de los servicios de un recurso que normalmente esperaría tener. Los ataques de DoS que el dispositivo puede soportar son ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack y Tear Drop.

TCP/IP/PORT/INTERFACE FILTER (Filtro)
Estas reglas ayudan en el filtrado de tráfico en la capa de red (es decir, en Layer 3). Cuando se crea una interfaz de encaminamiento, **Enable Firewall** debe estar marcado.
Navegue hasta Advanced Setup → Security → IP Filtering.

OUTGOING IP FILTER (Filtro IP de salida)
Ayuda en la configuración de reglas para rechazar (DROP) paquetes desde la interfaz LAN. Por defecto, si el cortafuegos está activado, se permite todo el tráfico IP que venga desde la LAN. Configurando uno o más filtros, los tipos de paquetes específicos que provengan de la LAN se podrán rechazar.

Ejemplo 1:

Filter Name	: Out_Filter1
Protocol	: TCP
Source IP address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 80
Dest. IP Address	: NA
Dest. Subnet Mask	: NA
Dest. Port	: NA

Este filtro rechazará todos los paquetes TCP provenientes de la LAN con dirección IP/Máscara de subred de 192.168.1.45/24 que tengan el puerto de destino 80 independientemente del destino. El resto de paquetes será aceptado.

Ejemplo 2:

Filter Name	: Out_Filter2
Protocol	: UDP
Source IP Address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 5060:6060
Dest. IP Address	: 172.16.13.4
Dest. Subnet Mask	: 255.255.255.0
Dest. Port	: 6060:7070

Este filtro rechazará todos los paquetes UDP provenientes de la LAN con dirección IP/Máscara de subred de 192.168.1.45/24 que tengan puertos de origen en el intervalo de 5060 a 6060 con destino 172.16.13.4/24 y con puertos de destino en el intervalo de 6060 a 7070.

INGOING IP FILTER (Filtro IP de entrada)
Ayuda a establecer reglas para permitir o denegar paquetes de la interfaz WAN. Por defecto, todo el tráfico IP de la WAN es bloqueado si el cortafuegos está activo. Configurando uno o más filtros, los tipos de paquetes específicos que provengan de la WAN se podrán aceptar.

Ejemplo 1:

Filter Name	: In_Filter1
Protocol	: TCP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 80
Dest. IP Address	: NA
Dest. Subnet Mask	: NA
Dest. Port	: NA
Selected WAN interface	: br0

Este filtro aceptará todos los paquetes TCP provenientes de la interfaz WAN "br0" con dirección IP/Máscara de subred 210.168.219.45/16 con Puerto de origen 80, independientemente del destino. El resto de paquetes de esta interfaz será RECHAZADO.

Ejemplo 2:

Filter Name	: In_Filter2
Protocol	: UDP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 5060:6060
Dest. IP Address	: 192.168.1.45
Dest. Sub. Mask	: 255.255.255.0
Dest. Port	: 6060:7070
Selected WAN interface	: br0

Esta regla Aceptará todos los paquetes UDP provenientes de la interfaz WAN "br0" con Dirección IP/Máscara de subred 210.168.219.45/16 y Puerto de origen en el intervalo de 5060 a 6060, con destino a 192.168.1.45/24 y con puerto de destino en el intervalo de 6060 a 7070. El resto de paquetes de esta interfaz será RECHAZADO.

MAC LAYER FILTER (Filtro MAC por capas)
Estas reglas ayudan en el filtrado del tráfico Layer 2. El Filtrado MAC solamente es efectivo en el modo Bridge. Tras crear una conexión en modo Bridge, navegue hasta Advanced Setup → Security → MAC Filtering en al interfaz Web de usuario.

Ejemplo 1:

Global Policy	: Forwarded
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: NA
Src. Interface	: eth1
Dest. Interface	: eth2

La inclusión de esta regla rechaza todas las tramas PPPoE que se transmiten desde eth1 a eth2 con dirección MAC de destino 00:12:34:56:78:90 independientemente de su dirección MAC de origen. El resto de tramas de esta interfaz será reenviado.

Ejemplo 2:

Global Policy	: Blocked
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: 00:34:12:78:90:56
Src. Interface	: eth1
Dest. Interface	: eth2

La inclusión de esta regla reenvía todas las tramas PPPoE que se transmiten desde eth1 a eth2 con dirección MAC de destino 00:12:34:56:78 y dirección MAC de origen 00:34:12:78:90:56. El resto de tramas de esta interfaz será rechazado.

Apéndice B - Asignación de PINs

Puertos ETHERNET (RJ45)

Puertos ETHERNET LAN (10/100Base-T)

Pin	Nombre de la señal	Definición de la señal
1	TXP	Transmisión de datos (positivo)
2	TXN	Transmisión de datos (negativo)
3	RXP	Recepción de datos (positivo)
4	NC	No utilizado
5	NC	No utilizado
6	RXN	Transmisión de datos (negativo)
7	NC	No utilizado
8	NC	No utilizado

Tabla 1

Señales para Puertos ETHERNET WAN (10/1001000Base-T)

Pin	Nombre de la señal	Definición de la señal
1	TRD+(0)	Transmisión/Recepción de datos 0 (positivo)
2	TRD-(0)	Transmisión/Recepción de datos 0 (negativo)
3	TRD+(1)	Transmisión/Recepción de datos 1 (positivo)
4	TRD+(2)	Transmisión/Recepción de datos 2 (positivo)
5	TRD-(2)	Transmisión/Recepción de datos 2 (negativo)
6	TRD-(1)	Transmisión/Recepción de datos 1 (negativo)

7	TRD+(3)	Transmisión/Recepción de datos 3 (positivo)
8	TRD-(3)	Transmisión/Recepción de datos 3 (negativo)

Tabla 2

Apéndice C - Especificaciones

Interfaz de Hardware

- RJ-11 X 1 para ADSL2
- RJ-45 X 4 para LAN (10/100 Base-T auto-sense)
- Reset Button X 1
- Power Switch X 1
- USB Host X 1
- Antena Wi-Fi fija de 2Bi x 2

Interfaz WAN

- ADSL2+ Bajada: 24 Mbps Subida: 1 Mbps
- ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2, AnnexM
- ADSL2 Bajada: 12 Mbps Subida: 1 Mbps

Interfaz LAN

- Standard IEEE 802.3, IEEE 802.3u
- Soporte MDI/MDX Sí
- 10/100 BaseT Auto-sense

Interfaz Wireless

- IEEE802.11b/g/n
- 64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption/ WPA/WPA2 encryption
- 11 Canales (US, Canadá)/ 13 Canales (Europa)/ 14 Canales (Japón)
- Tasa de datos de hasta 300Mbps
- WPA/WPA2 Sí
- IEEE 802.1x Sí
- Frecuencia de funcionamiento RF 2.412-2.497GHz (Genérico, 2.4GHz ISM Band),
- 2.400-2.4835GHz (Egipto, 2.4GHz ISM Band).
- WMM Sí

Gestión

- Compatible con los protocolos de gestión remota TR-069/TR-098/TR-111, Telnet, gestión basada en Web, Copia de seguridad y su restablecimiento.
- Actualización de software vía servidor HTTP / TFTP

Protocolos de red

- Cápsulas RFC2684 VC-MUX, LLC/SNAP para bridged o paquetes enrutados
- RFC2364 PPP sobre AAL5
- IPoA, PPPoA, PPPoE, PPPoE pass-through independientes
- PPPoE filtrado de paquetes on-PPPoE entre WAN and LAN
- Puente transparente entre todas las interfaces LAN y WAN
- Soporta VLAN 802.1p/802.1q
- Algoritmo de árbol de expansión (Spanning Tree)
- Proxy IGMP V1/V2/V3, Snooping IGMP V1/V2/V3, Desasociado rápido
- Encaminamiento rápido RIP v1/v2, ARP, RARP, SNTP, Servidor/Cliente /Relay DHCP

- DNS Relay, Dynamic DNS,
- IPv6 subset

Funciones de seguridad

- Reglas de filtrado PAP, CHAP, TCP/IP/Puerto
- Port Triggering (Redireccionamiento de puertos)
- Filtrado de paquetes y direcciones MAC, Control de acceso, acceso SSH

QoS

- L3 basado en políticas QoS, IP QoS, ToS

Firewall/Filtering (Cortafuegos/Filtros)

- Cortafuegos de inspección de todos los estados
- Filtro de paquete sin estado
- Denial of Service (DOS): ARP attacks, Ping attacks, Ping of Death, LAND,SYNC, Smurf, Unreachable, Teardrop
- Reglas de filtrado TCP/IP/Port/interface soportan tanto filtros de entrada como de salida.

NAT/NAPT

- Soporta Port Triggering y Port forwarding
- Puerto de sobrecarga simétrico NAT, Full-Cone NAT
- Dynamic NAPT (NAPT N-to-1)
- Soporta DMZ host
- Virtual Servers (Servidores virtuales)
- VPN Passthrough (PPTP, L2TP, IPSec)

Aplicación Passthrough

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box, etc.

Alimentación ..... Entrada: 100 - 240 Vac
Salida: 12 Vdc / 1 A

Temperatura ambiente

Temperatura de funcionamiento ..... 0 ~ 40 grados centígrados
Temperatura de almacenaje.....-20 ~ 70 grados centígrados
Humedad relativa..... 5 ~ 95% (sin condensación)

Dimensiones.....142 mm (L) x 30 mm (Al) x 125 mm (An)

Certificaciones..... CE, Wi-Fi 11n

Peso

(1*AR-5387un, 1*cable RJ14, 1*cable RJ45, 1*adaptador de corriente, 2*Microfiltros, 1*conector en T, 1*CD-ROM) = 0.45 Kg aprox.

NOTA: Estas especificaciones están sujetas a cambios sin previo aviso.

Apéndice D – Cliente SSH

Al contrario que Microsoft Windows, Linux OS incluye un cliente ssh. Para los usuarios de Windows existe un dominio público de nombre "putty" desde donde puede descargarse:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Para acceder al cliente ssh primero hay que activar el acceso SSH para la LAN o WAN desde el menú Management → Access Control → Services en la interfaz Web de usuario.

Para acceder al router usando el cliente ssh de Linux

Para el acceso a la LAN, escriba: ssh -l admin 192.168.1.1

Para el acceso a la WAN, escriba: ssh -l support *WAN IP address*

Para acceder al router usando el cliente ssh "putty" de Windows

Para el acceso a la LAN, escriba: putty -ssh -l admin 192.168.1.1

Para el acceso a la WAN, escriba: putty -ssh -l support *WAN IP address*

NOTA: La dirección IP WAN puede encontrarse en la pantalla Device Info → WAN

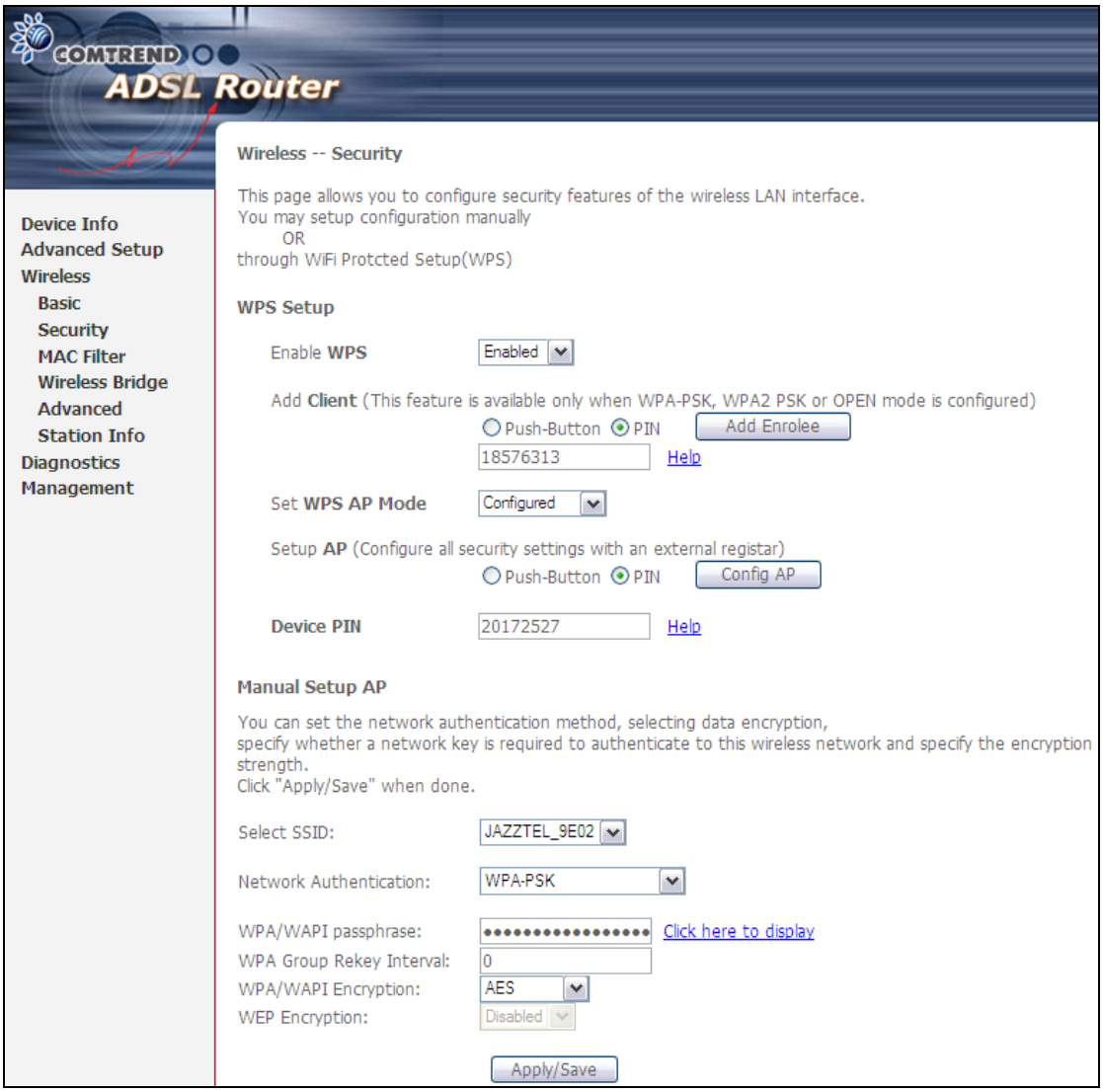
Apéndice E – Funcionamiento WPS

Esta sección muestra el proceso básico de AP WPS Operation.

E1 Incorporación del abonado con el método PIN

1) Seleccione la opción "Pin"
2) Introduzca el Pin desde la estación del abonado (20172527 en este ejemplo)

3) Haga clic en **Add Enrollee** (Añadir Abonado)



4) Accione la Estación para comenzar la incorporación del Abonado WPS.

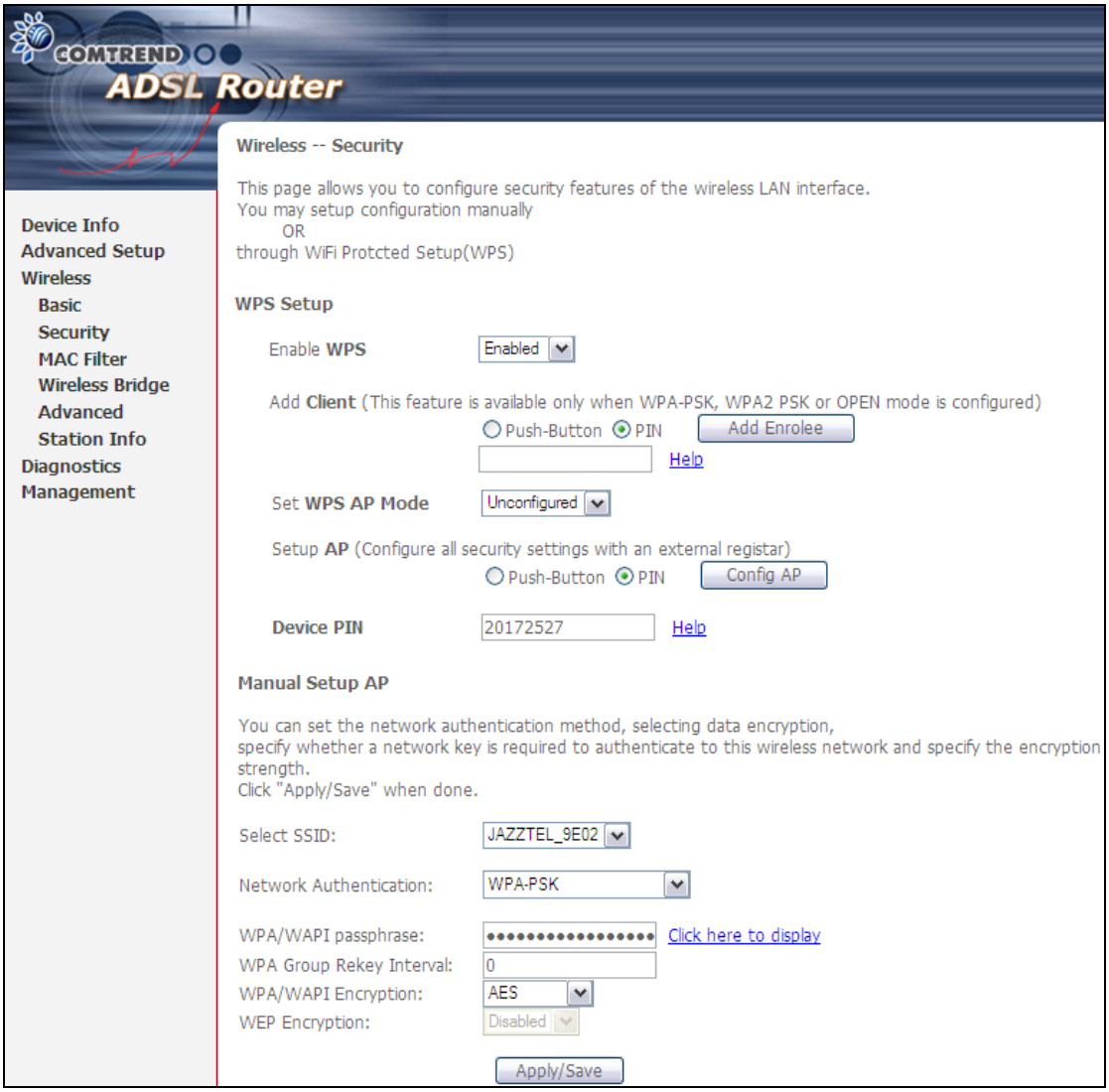
E2 Incorporación del abonado con el método PBC

1) Seleccione la opción “Push-Button” y haga clic en añadir Abonado.

2) Accione la Estación para comenzar la incorporación del Abonado WPS.

E3 Configuración del punto de acceso (PA)

1) Establezca PA como "Unconfigured Mode" (Modo desconfigurado) y haga clic en el botón **Config AP** (configurar PA).



2) Lea el número PIN del dispositivo (20172527 en este ejemplo) e introdúzcalo en el External Registrar (ER) cuando el ER pida el número PIN del dispositivo. El ER puede ser con cable (por ejemplo en Windows Vista) o inalámbrico (Estación Intel).

3) Actualice la página Web una vez que ER haya completado la configuración del PA para comprobar la configuración de los parámetros.

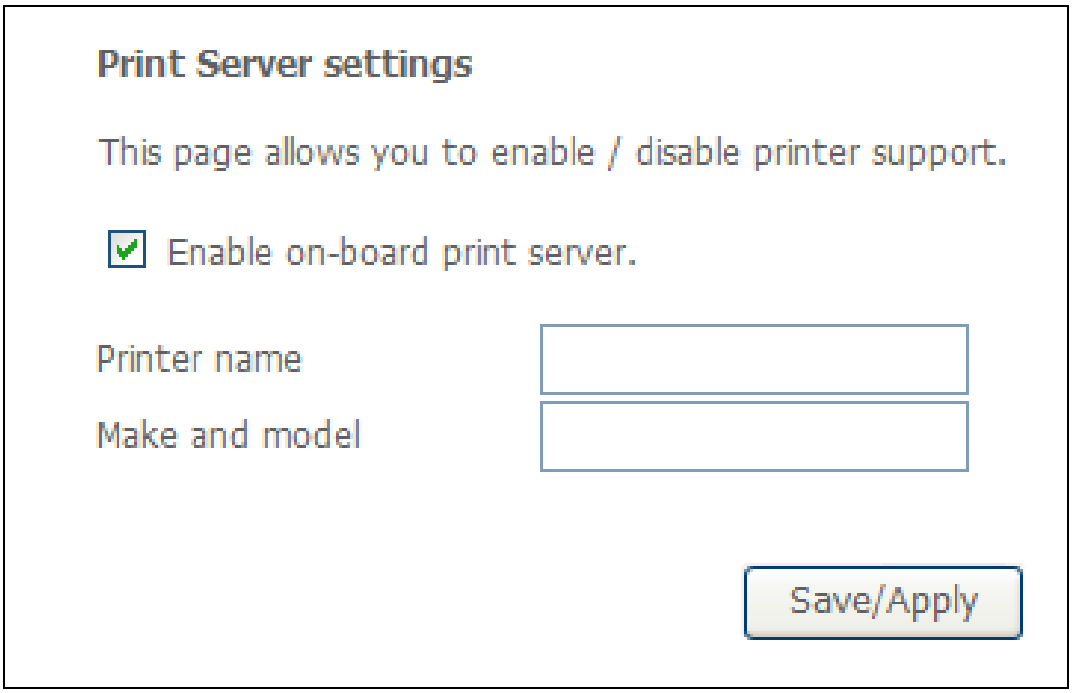
Apéndice F – Servidor de impresión

Estos pasos explican el procedimiento para activar el servidor de impresión.

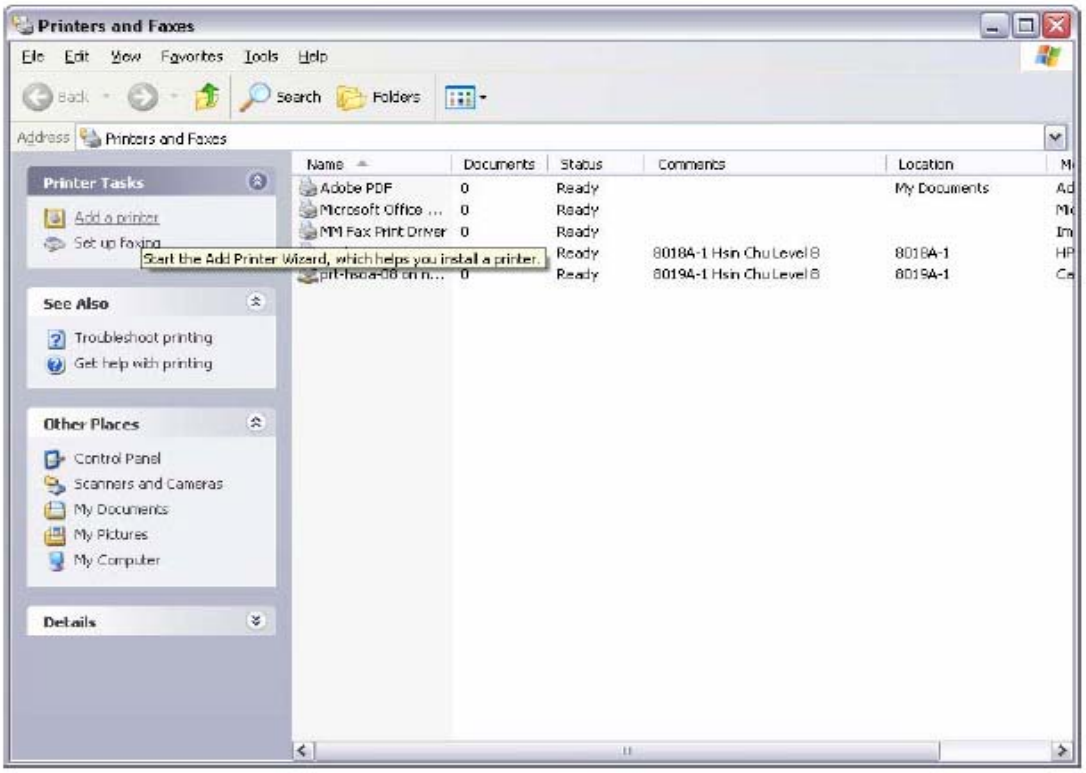
NOTA:	Esta función sólo se aplica a los modelos con Puerto Host USB.

PASO 1: Active el servidor de impresión desde la interfaz Web de usuario. Marque la casilla Enable on-board print server ☑ e introduzca el nombre de la impresora y el fabricante del modelo.

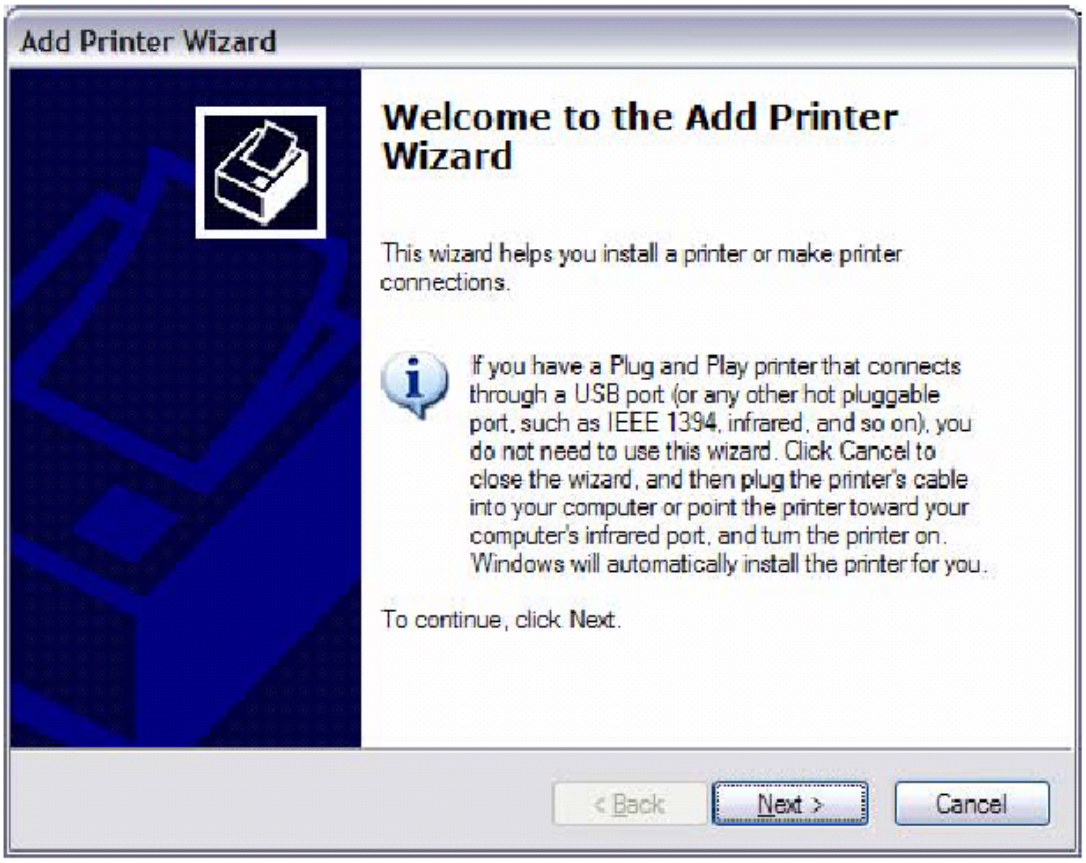
NOTA:	El **Printer name** (nombre de la impresora) puede ser cualquier cadena de texto hasta 40 caracteres. El **Make and model** (fabricante y modelo) puede ser una cadena de texto de hasta 128 caracteres.



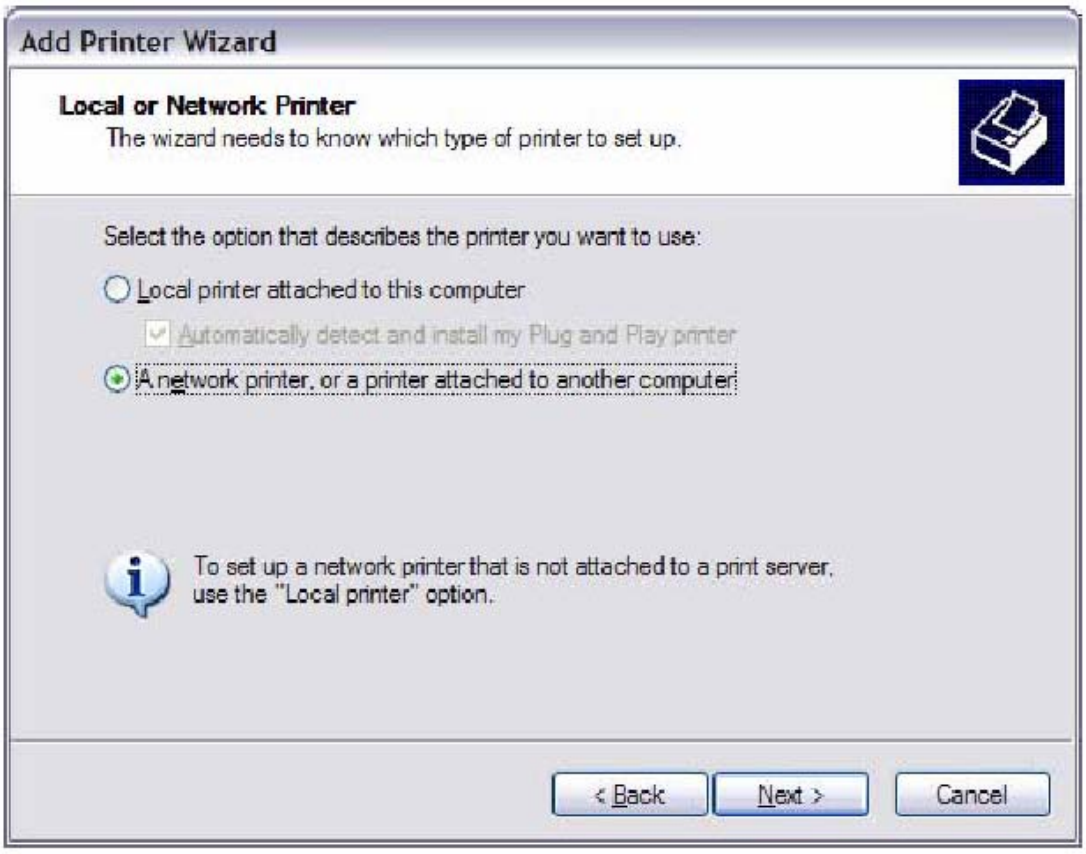
PASO 2: Diríjase a la aplicación **Impresoras y faxes** en el **Panel de Control** y seleccione la función **Agregar impresora** (como se muestra en el menú lateral inferior).



PASO 3: Haga clic en **Next** para continuar una vez que se le muestre el diálogo de la imagen inferior.


Add Printer Wizard
Welcome to the Add Printer Wizard
This wizard helps you install a printer or make printer connections.
If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.
To continue, click Next.
< Back
Next >
Cancel

PASO 4: Seleccione **Impresora de Red** y haga clic en **Siguiente**

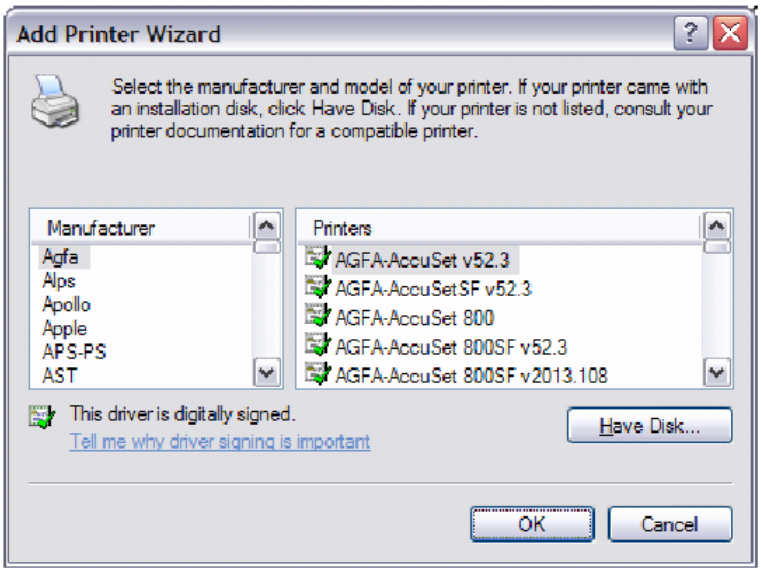

Add Printer Wizard
Local or Network Printer
The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use:
Local printer attached to this computer
Automatically detect and install my Plug and Play printer
A network printer, or a printer attached to another computer
To set up a network printer that is not attached to a print server, use the "Local printer" option.
< Back
Next >
Cancel

PASO 5: Seleccione **Conectar a una impresora en Internet** e introduzca el enlace a su impresora.
(p. ej. http://192.168.1.1:631/printers/hp3845) y haga clic en **siguiente.**

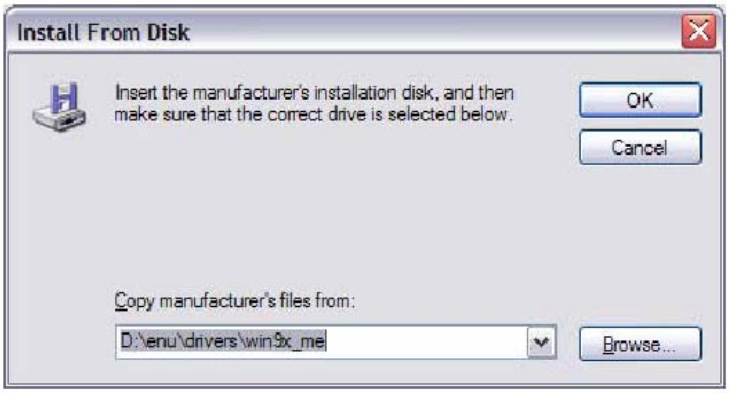
NOTA:	El nombre de la impresora debe ser el mismo nombre introducido en la interfaz de usuario del módem ADSL en el paso 1 de la sección Configuración del servidor de impresión.

Add Printer Wizard
Specify a Printer
If you don't know the name or address of the printer, you can search for a printer that meets your needs.
What printer do you want to connect to?
Find a printer in the directory
Connect to this printer (or to browse for a printer, select this option and click Next):
Name:
Example: \\server\printer
Connect to a printer on the Internet or on a home or office network:
URL:
http://192.168.1.1:631/printers/hp3845
Example: http://server/printers/myprinter/.printer
< Back
Next >
Cancel

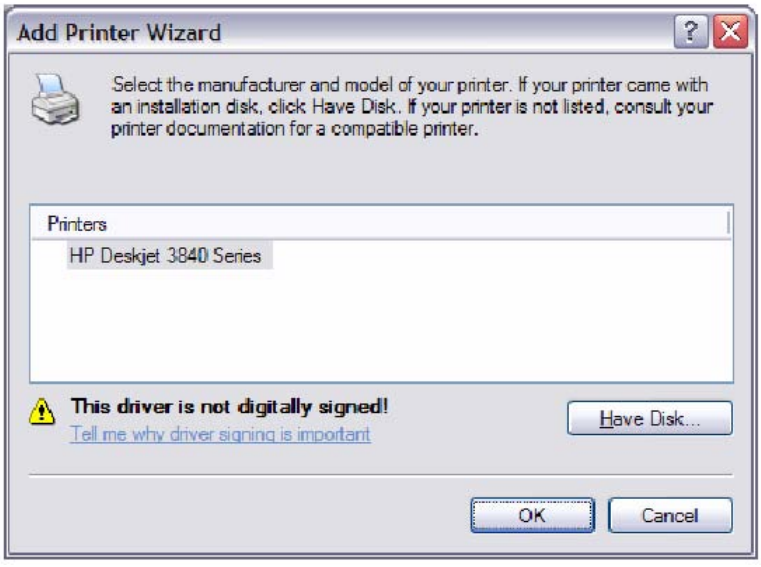
PASO 6: Haga clic en **Tengo disco** e inserte el CD con los drivers de la impresora.



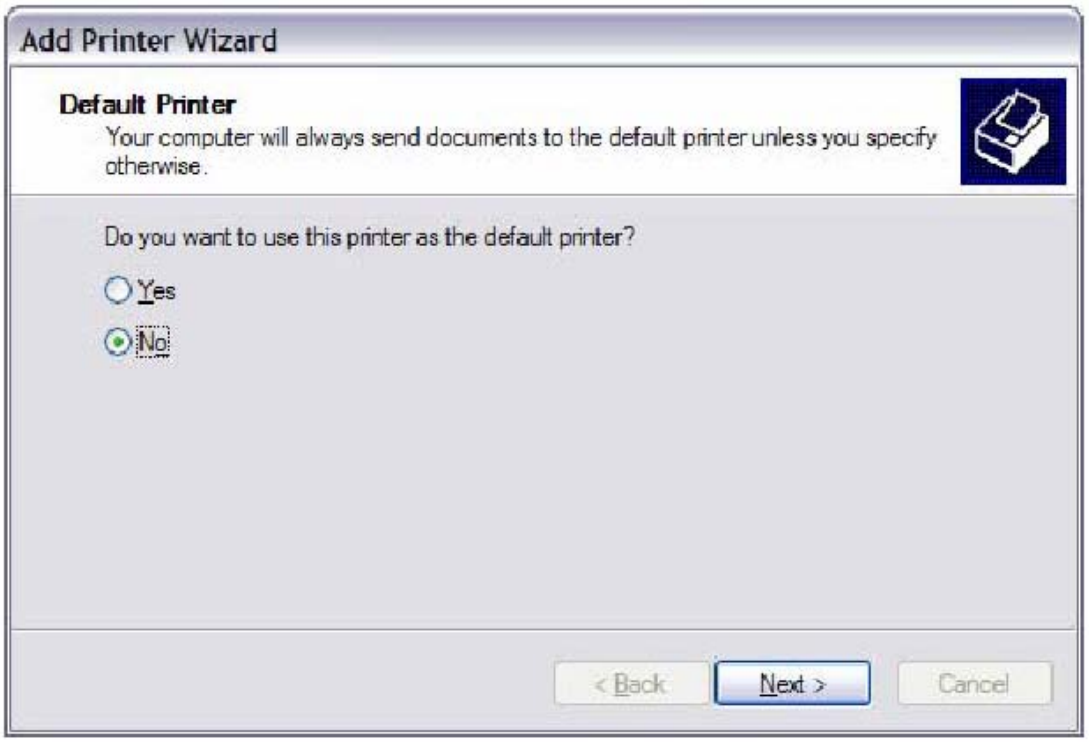
PASO 7: Seleccione la carpeta con el controlador en el CD-ROM y haga clic en **Aceptar.**



PASO 8: Una vez que aparezca el nombre de la impresora, haga clic en **Aceptar.**

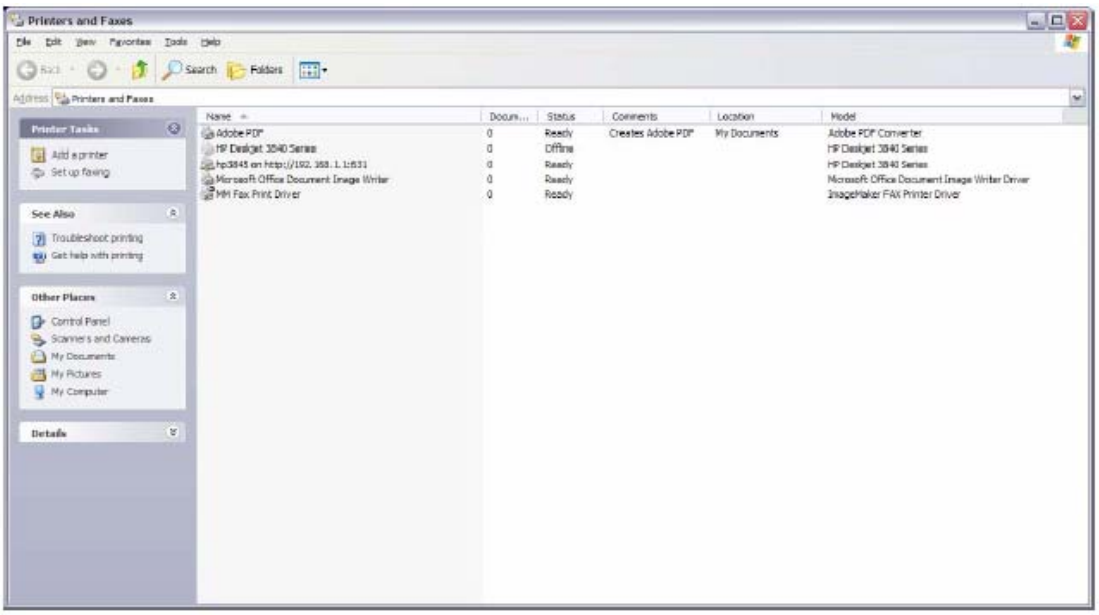

Add Printer Wizard
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.
Printers
HP Deskjet 3840 Series
This driver is not digitally signed!
Tell me why driver signing is important
Have Disk...
OK
Cancel

PASO 9: Escoja **Sí** o **No** para configurarla como impresora predeterminada y haga clic en **Siguiente.**


Add Printer Wizard
Default Printer
Your computer will always send documents to the default printer unless you specify otherwise.
Do you want to use this printer as the default printer?
Yes
No
< Back
Next >
Cancel

PASO 10: Haga clic en .

PASO 11: Compruebe el estado de la impresora desde el Panel de Control de Windows en la ventana Impresora. El estado debería aparecer como **Listo**.



Apéndice G – Instalación de la conexión

Crear una conexión WAN es un proceso que se realiza en dos etapas.

1 – Configurar un interfaz Layer 2 (ATM).
2 – Añadir una conexión WAN a la interfaz Layer 2.

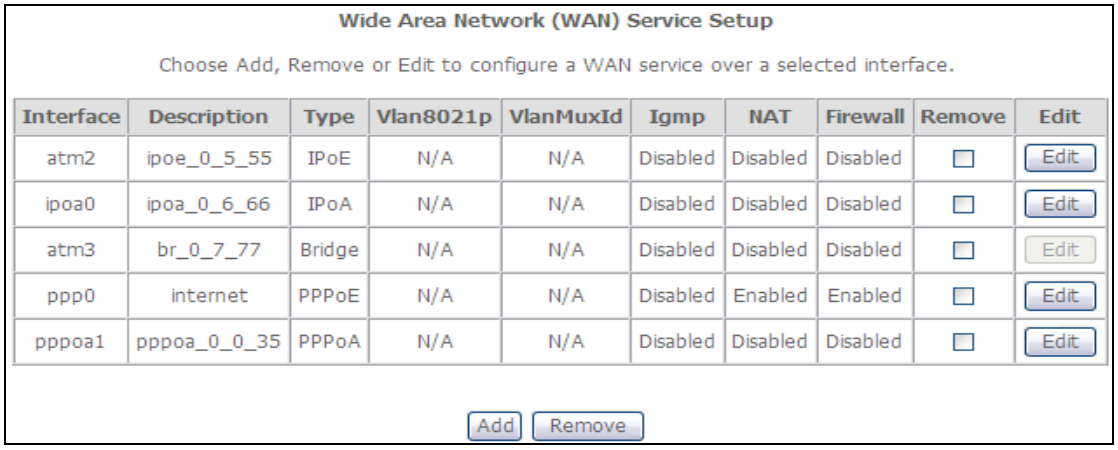
En las siguientes secciones se describe cada etapa paso a paso.

G1 ~ Interfaces Layer 2

Cada interfaz Layer 2 opera en uno de estos modos: Default, VLAN Mux o MSC. Como introducción se incluye una pequeña descripción de cada uno de estos tres modos. Es importante entender las diferencias entre estos modos de conexión, ya que determinan el número y tipo de conexiones que pueden configurarse.

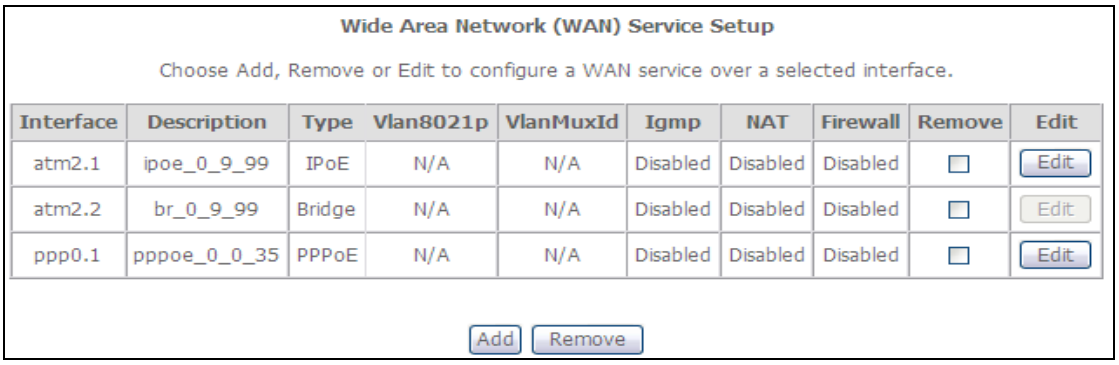
MODO DEFAULT (PREDETERMINADO)

En este modo existe una relación 1:1 entre las interfaces y las conexiones WAN, en el sentido en que una interfaz en el modo default soporta únicamente una conexión. Sin embargo, al contrario que en los modos multiconexión descritos más abajo, soporta los cinco tipos de conexión.
La imagen muestra los cinco tipos de conexión disponibles en el modo default ATM.
NOTA: El tipo de enlace EoA es para PPPoE, IPoE y Bridge.


Wide Area Network (WAN) Service Setup
Choose Add, Remove or Edit to configure a WAN service over a selected interface.
Interface Description Type Vlan8021p VlanMuxId Igmp NAT Firewall Remove Edit
atm2 ipoe_0_5_55 IPoE N/A N/A Disabled Disabled Disabled Edit
ipoa0 ipoa_0_6_66 IPoA N/A N/A Disabled Disabled Disabled Edit
atm3 br_0_7_77 Bridge N/A N/A Disabled Disabled Disabled Edit
ppp0 internet PPPoE N/A N/A Disabled Enabled Enabled Edit
pppoa1 pppoa_0_0_35 PPPoA N/A N/A Disabled Disabled Disabled Edit
Add Remove

MODO VLAN MUX

Este modo utiliza el etiquetaje VLAN para permitir múltiples conexiones sobre una única interfaz. Las conexiones PPPoE, IPoE y Bridge son soportadas, mientras que las conexiones PPPoA y IPoA no se permiten.
La imagen inferior muestra las múltiples conexiones sobre una única interfaz VLAN Mux.

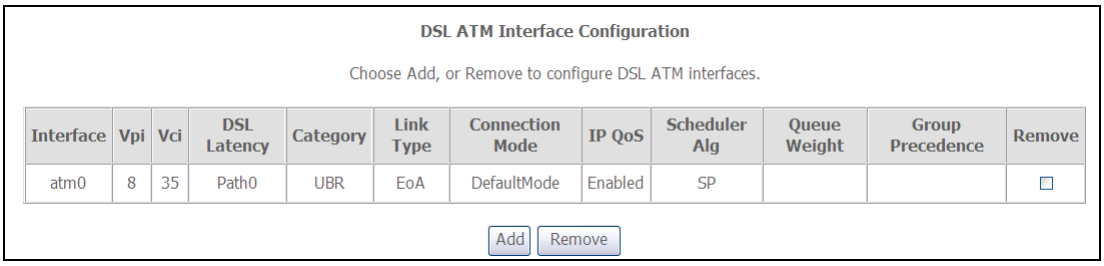

Wide Area Network (WAN) Service Setup
Choose Add, Remove or Edit to configure a WAN service over a selected interface.
Interface Description Type Vlan8021p VlanMuxId Igmp NAT Firewall Remove Edit
atm2.1 ipoe_0_9_99 IPoE N/A N/A Disabled Disabled Disabled Edit
atm2.2 br_0_9_99 Bridge N/A N/A Disabled Disabled Disabled Edit
ppp0.1 pppoe_0_0_35 PPPoE N/A N/A Disabled Disabled Disabled Edit
Add Remove

G1.1 Interfaces ATM

Siga los siguientes procedimientos para configurar una interfaz ATM.

NOTA:	El AR-5387un soporta hasta 16 interfaces ATM.

PASO 1: Vaya a Advanced Setup → Layer2 Interface → ATM Interface.

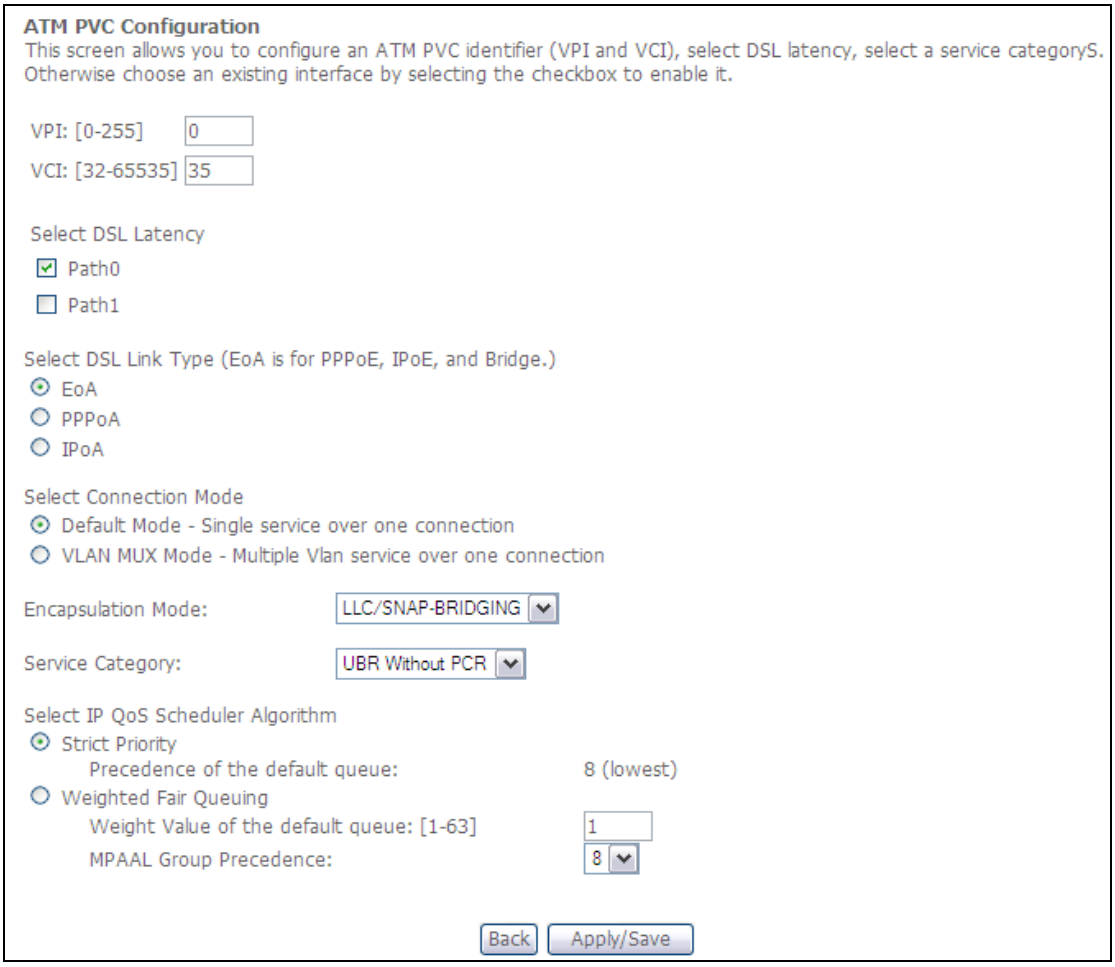

DSL ATM Interface Configuration
Choose Add, or Remove to configure DSL ATM interfaces.
Interface Vpi Vci DSL Latency Category Link Type Connection Mode IP QoS Scheduler Alg Queue Weight Group Precedence Remove
atm0 8 35 Path0 UBR EoA DefaultMode Enabled SP
Add Remove

La tabla siguiente se muestra para facilitar la consulta.

Encabezado	**Descripción**
Interface	Nombre de la interfaz WAN.
VPI	ATM VPI (0-255)
VCI	ATM VCI (32-65535)
DSL Latency	{Path0} → port ID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
Category	Categoría de servicio ATM
Link Type	Seleccione EoA (para PPPoE, IPoE y Bridge), PPPoA o IPoA.
Connection Mode	Default Mode - Servicio único sobre una conexión Vlan Mux Mode – Múltiples servicios Vlan sobre una conexión
IP QoS	Estado de Calidad del Servicio (QoS)
Scheduler Alg	El algoritmo usado para programar el comportamiento de la cola.
Queue Weight	El peso de una cola específica.
Group Precedence	La Precedencia del grupo específico.
Remove	Seleccionar elementos para eliminarlos

PASO 2: Haga clic sobre **Add** para ver la siguiente pantalla.

NOTA:	Para añadir conexiones WAN a un tipo de interfaz debe borrar las conexiones existentes desde otro tipo de interfaz usando para ello el botón **Remove**.


ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS. Otherwise choose an existing interface by selecting the checkbox to enable it.
VPI: [0-255] 0
VCI: [32-65535] 35
Select DSL Latency
Path0
Path1
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
EoA
PPPoA
IPoA
Select Connection Mode
Default Mode - Single service over one connection
VLAN MUX Mode - Multiple Vlan service over one connection
Encapsulation Mode: LLC/SNAP-BRIDGING
Service Category: UBR Without PCR
Select IP QoS Scheduler Algorithm
Strict Priority
Precedence of the default queue: 8 (lowest)
Weighted Fair Queuing
Weight Value of the default queue: [1-63] 1
MPAAL Group Precedence: 8
Back
Apply/Save

Hay varias configuraciones aquí, incluyendo: VPI/VCI, DSL Latency, DSL Link Type, Encapsulation Mode, Service Category, Connection Mode y Quality of Service.

La tabla inferior muestra la disponibilidad del tipo de enlace xDSL con cada modo de conexión.

	Tipo de enlace xDSL		
Modo de conexión	EoA*	PPPoA	IPoA
Default Mode	OK	OK	OK
VLAN Mux Mode	OK	X	X

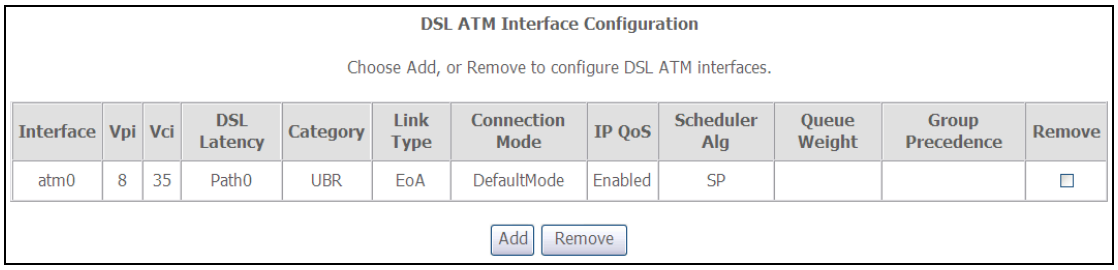
EoA incluye los tipos de conexión PPPoE, IPoE y Bridge.

Aquí se muestran las distintas encapsulaciones para cada tipo de enlace xDSL:

- EoA- LLC/SNAP-BRIDGING, VC/MUX
- PPPoA- VC/MUX, LLC/ENCAPSULATION
- IPoA- LLC/SNAP-ROUTING, VC MUX

PASO 3: Haga clic sobre **Apply / Save** para confirmar su elección.

En la siguiente pantalla compruebe que la interfaz ATM ha sido añadida a la lista. Por ejemplo, en la imagen inferior se muestra una interfaz ATM en PVC 0/35 en modo Default con tipo de enlace EoA.



DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove
atm0	8	35	Path0	UBR	EoA	DefaultMode	Enabled	SP			☐

Add Remove

Para añadir una conexión WAN, vaya a la sección G2 ~ Conexiones WAN.

La tabla siguiente se muestra para facilitar la consulta.

Encabezado	**Descripción**
Interface	Nombre de la interfaz WAN.
DSL Latency	{Path0} → port ID = 0 {Path1} → port ID = 1 {Path0&1} → port ID = 4
PTM Priority	Normal o Alta Prioridad (Prevención)
Modo de conexión	Default Mode - Servicio único sobre una interfaz. Vlan Mux Mode – Múltiples servicios Vlan sobre una interfaz.
IP QoS	Estado de Calidad de Servicio (QoS).
Scheduler Alg	El algoritmo utilizado para programar el comportamiento de la cola.
Queue Weight	El peso de la cola especificada.
Group Precedence	La precedencia del grupo especificado.
Remove	Selecciona las interfaces para eliminar

PASO 5: Haga clic sobre **Add** para ver la siguiente pantalla.

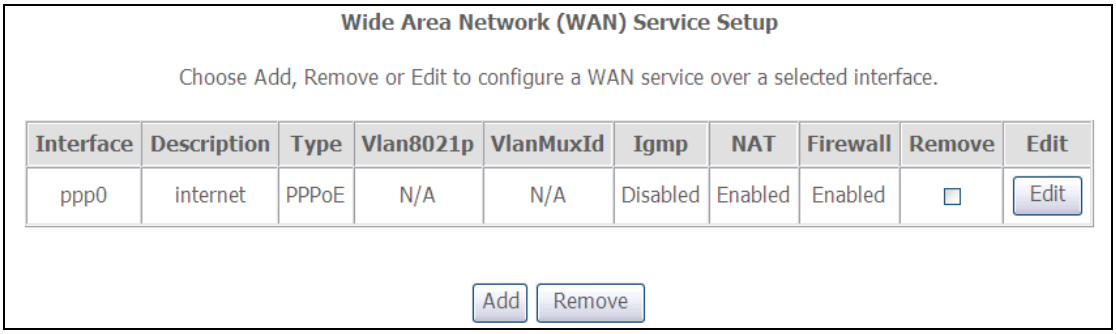
NOTA:	Para añadir conexiones WAN a un tipo de interfaz debe borrar las conexiones existentes desde otro tipo de interfaz usando para ello el botón **Remove**.

G2 ~ Conexiones WAN

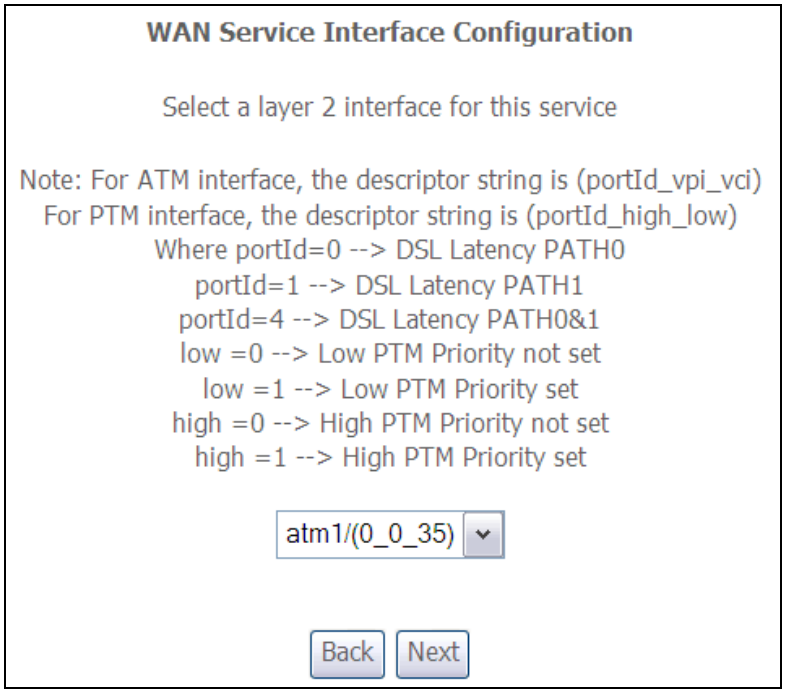
En el modo Default el AR-5387un soporta una conexión WAN para cada interfaz y hasta un máximo de 8 conexiones. VLAN Mux y MSC soportan hasta 16 conexiones.

Para configurar una conexión WAN siga las siguientes instrucciones.

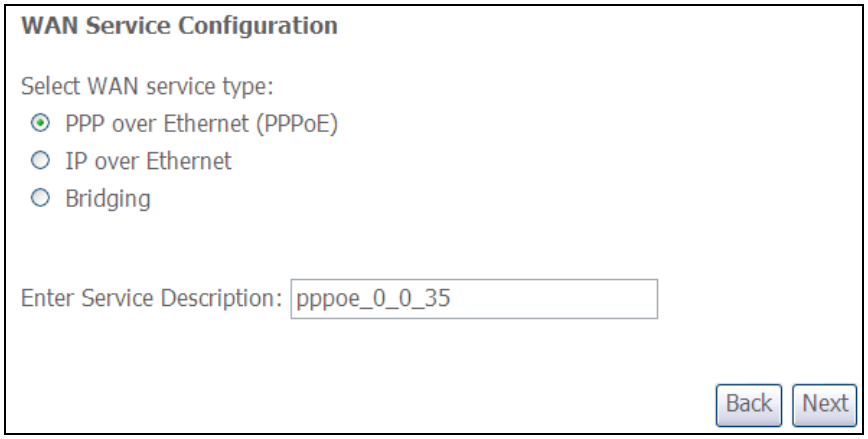
PASO 1: Diríjase a la pantalla Advanced Setup → WAN Service.



PASO 2: Haga clic sobre el botón **Add** para crear una nueva conexión WAN. Aparecerá la siguiente pantalla.

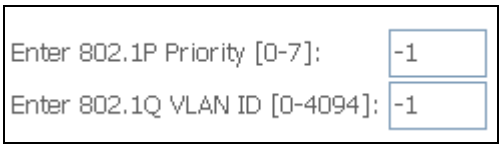

WAN Service Interface Configuration
Select a layer 2 interface for this service
Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set
atm1/(0_0_35)
Back
Next

PASO 3: Seleccione una interfaz layer 2 desde la caja desplegable y haga clic en **Next**.
La pantalla WAN Service Configuration debería aparecer como se muestra a continuación.



NOTA:	Los servicios WAN mostrados aquí son los soportados por la interfaz layer 2 que ha seleccionado en el paso anterior. Si desea cambiar su selección haga clic sobre el botón **Back** y seleccione una interfaz layer 2 diferente.

PASO 4: Para las conexiones VLAN Mux solamente deberá introducir etiquetas Priority y VLAN ID.



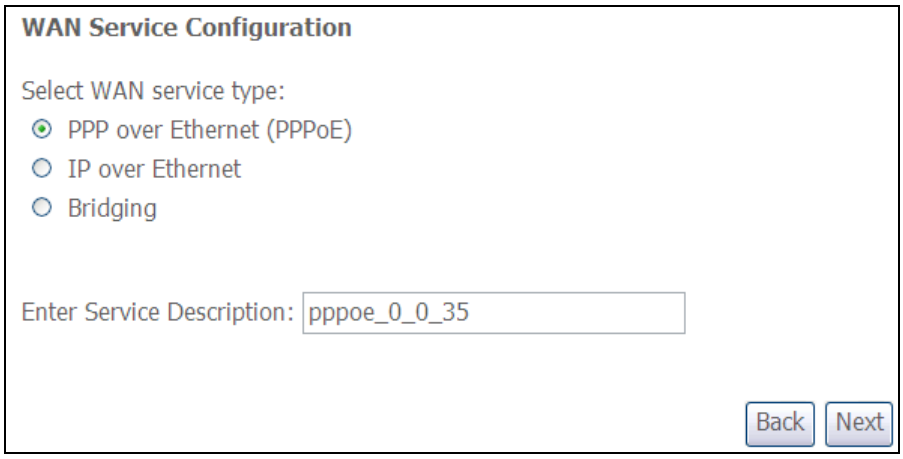
PASO 5: Ahora siga las instrucciones específicas para el tipo de servicio WAN que desea establecer. Esta lista debería ayudarle a localizar el procedimiento correcto:

(1) Para G2.1 PPP over ETHERNET (PPPoE), vaya a la página 107.
(2) Para G2.2 PPP over ETHERNET (IPoE), vaya a la página 111.
(3) Para G2.3 Bridging (Puenteado), vaya a la página 115.
(4) Para G2.4 PPP over ATM (PPPoA), vaya a la página 116.
(5) Para G2.5 IP over ATM (IPoA), vaya a la página 120.

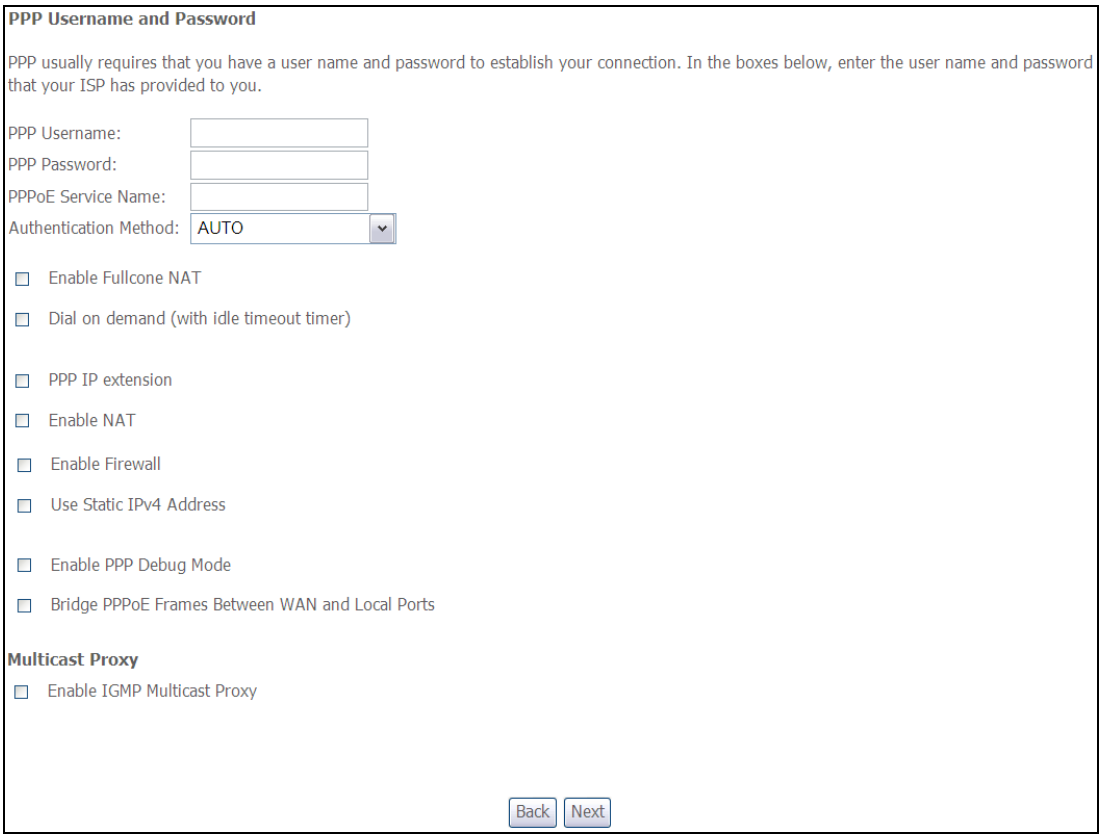
Los apartados que siguen continúan el procedimiento de configuración del servicio WAN.

G2.1 PPP over ETHERNET (PPPoE)

PASO 1: Seleccione el botón de activación PPP over Ethernet y haga clic en **Next**. También puede activar IPv6 marcando la casilla ☑ en la parte inferior de la pantalla.



PASO 2: En la siguiente pantalla, introduzca la configuración PPP proporcionada por su ISP (proveedor de servicios).
Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.

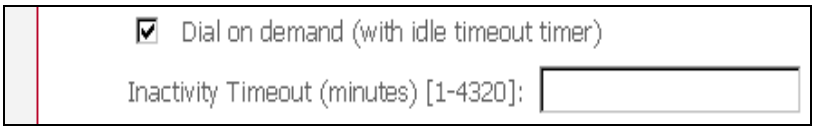

PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method: AUTO
Enable Fullcone NAT
Dial on demand (with idle timeout timer)
PPP IP extension
Enable NAT
Enable Firewall
Use Static IPv4 Address
Enable PPP Debug Mode
Bridge PPPoE Frames Between WAN and Local Ports
Multicast Proxy
Enable IGMP Multicast Proxy
Back
Next

Los ajustes mostrados arriba se describen a continuación.

PPP SETTINGS
El nombre de usuario y contraseña PPP dependen de los requerimientos del ISP. El nombre de usuario puede tener un máximo de 256 caracteres y la contraseña un máximo de 32 caracteres de longitud. Para el método de Autentificación, elija entre AUTO, PAP, CHAP y MSCHAP.

ENABLE FULLCONE NAT
Esta opción se muestra accesible cuando está activado NAT. Conocida como NAT uno-a-uno, todas las peticiones desde la misma dirección IP y puerto interno son mapeadas a la misma dirección IP y puerto externo. Un host externo puede enviar un paquete a un host interno, enviando el paquete a la dirección externa mapeada.

DIAL ON DEMAND
El AR-5387un se puede configurar de manera que se desconecte si no existe actividad durante un periodo de tiempo determinado marcando la casilla Dial on Demand ☑. También se debe introducir un periodo de tiempo de inactividad dentro del intervalo de 1 a 4320 minutos.



PPP IP EXTENSION
La extensión PPP IP es una función especial implementada por algunos proveedores de servicios. A menos que su proveedor de servicios requiera específicamente esta configuración, no la seleccione.

La extensión PPP IP hace lo siguiente:

- Solamente permite un PC en la LAN.
- Desactiva NAT y Firewall.
- El dispositivo se convierte en la pasarela predeterminada y en el servidor DNS del PC a través de DHCP y mediante el uso de la dirección IP de la interfaz LAN.
- El dispositivo extiende la subred IP al proveedor de servicios remoto del PC de la LAN, es decir, el PC se convierte en un host perteneciente a la misma subred IP.
- El dispositivo puentea los paquetes IP entre la WAN y los puertos LAN a no ser que el paquete sea dirigido a la dirección IP de los dispositivos LAN.
- La dirección IP pública asignada desde el lado remoto usando el protocolo PPP/IPCP no se utiliza de momento en la interfaz WAN PPP. En su lugar, es reenviada a la interfaz del PC de la LAN a través de DHCP. Solamente un PC de la LAN puede conectarse de forma remota, ya que el servidor DHCP dentro del dispositivo solamente posee una dirección IP para asignar a un dispositivo de LAN.

ENABLE NAT
Si la LAN está configurada con una dirección IP privada, el usuario debería marcar esta casilla ☑. El submenú NAT aparecerá en el menú Advanced Setup tras reiniciar. Por otro lado, si no se utiliza una dirección IP privada (p. ej. la LAN utiliza una IP pública), esta casilla ☑ no debería seleccionarse para liberar recursos del sistema y lograr un mejor rendimiento.

ENABLE FIREWALL
Si esta casilla ☑ está seleccionada se mostrará el submenú Security en el menú Advanced Setup tras el reinicio. Si el firewall no es necesario, esta casilla ☑ no debería seleccionarse para liberar recursos del sistema y lograr un mejor rendimiento.

USE STATIC IPv4 ADDRESS
A menos que su proveedor de servicios lo requiera expresamente, no selecione la casilla ☑. En caso de que debe seleccionarla, introduzca la dirección de IP estática en el campo IPv4 Address. No olvide ajustar la configuración de la IP en Static IP Mode como se describe en 3.2 Configuración IP.

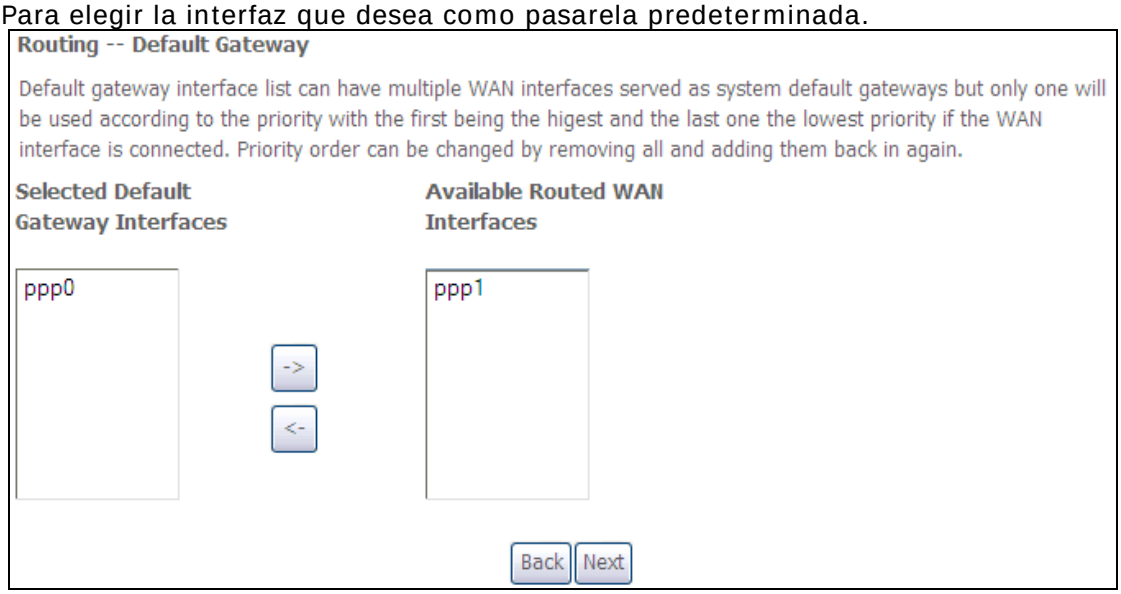
ENABLE PPP DEBUG MODE
Cuando se selecciona esta opción el sistema incluye más información sobre la conexión PPP en el sistema de registro. Esta función está indicada para la depuración de errores y no para un uso normal.

BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS
(Esta opción aparece oculta cuando está activo PPP IP Extension)
Cuando se activa se crean conexiones locales PPPoE en el entorno de la WAN. Active esta opción solamente si los dispositivos del entorno de la LAN están ejecutando clientes PPPoE, de lo contrario desactívela. El AR-5387un soporta sesiones pass-through PPPoE desde el entorno de la LAN mientras ejecuta un cliente simultáneamente desde dispositivos LAN non-PPPoE.

ENABLE IGMP MULTICAST PROXY
Marque la casilla ☑ para activar Group Membership Protocol (IGMP) multidifusión. Este protocolo es utilizado por los host IPv4 para informar a cualquier router multidifusión cercano de los grupos multidifusión que tiene abonados.

PASO 3:

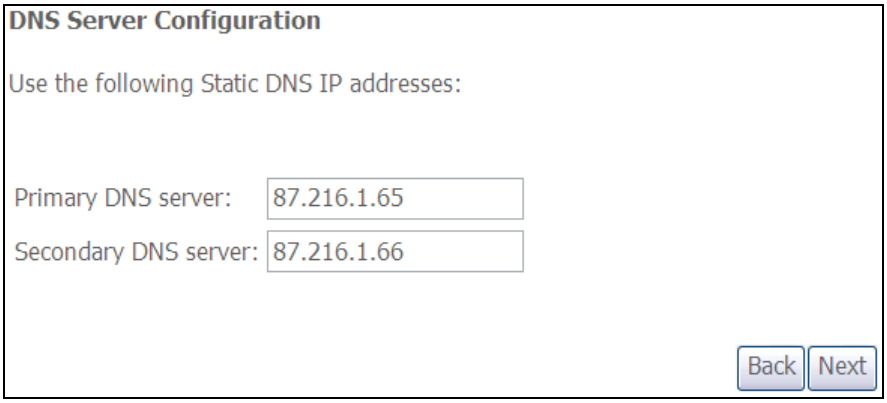
Para elegir la interfaz que desea como pasarela predeterminada.


Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
ppp0
ppp1
->
<-
Back
Next

Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.

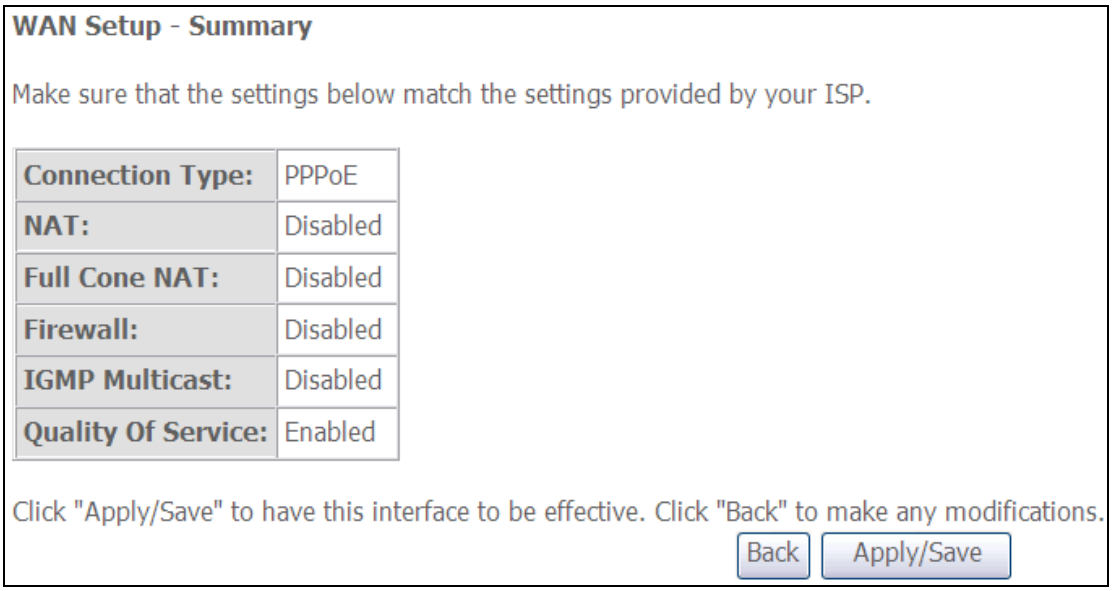
PASO 4:

Para establecer una dirección IP que el CPE usará para trasmitir la query DNS.



Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.

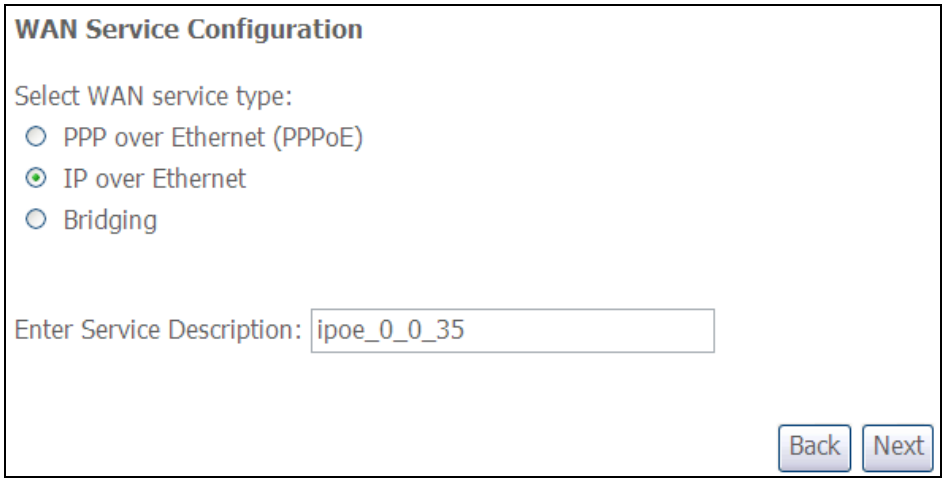
PASO 5: La pantalla WAN Setup - Summary muestra una vista general del servicio WAN que usted ha configurado. Compruebe los ajustes y haga clic sobre **Apply / Save** si son correctos, o haga clic en **Back** para modificarlos.


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: PPPoE
NAT: Disabled
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

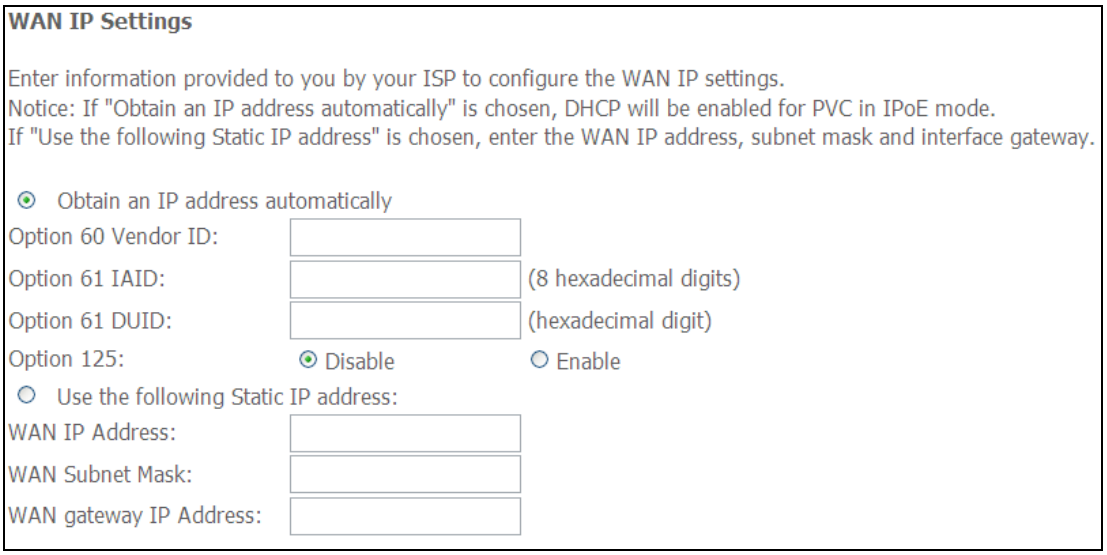
Tras hacer clic sobre **Apply / Save**, el nuevo servicio aparecerá en la pantalla principal.
Para activarlo debe reiniciar el equipo. Diríjase a Management → Reboot y haga clic en **Reboot.**

G2.2 PPP over ETHERNET (IPoE)

PASO 1: Seleccione el botón de activación IP over Ethernet y haga clic en **Next**. También puede activar IPv6 marcando la casilla ☑ en la parte inferior de la pantalla.

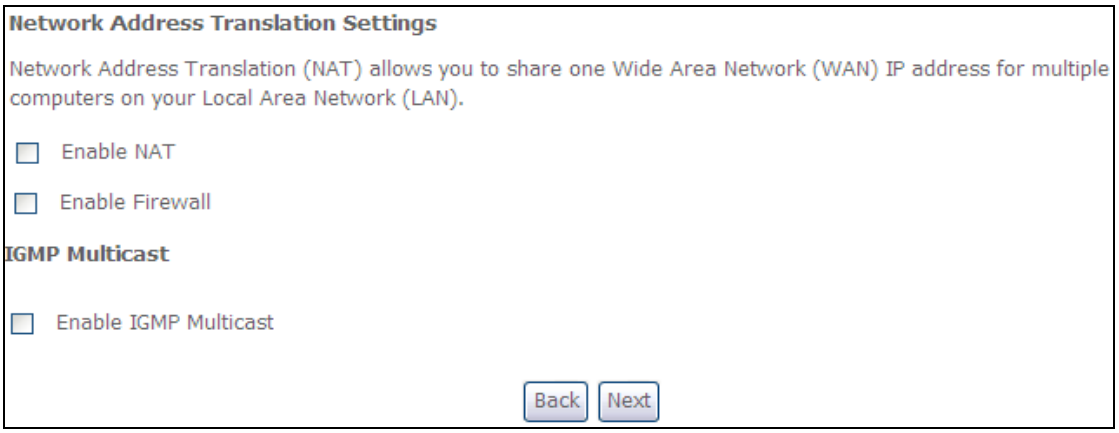


PASO 2: La pantalla de configuración WAN IP proporciona acceso a los ajustes del servidor DHCP.
Puede seleccionar el botón de activación **Obtain an IP address automatically** para activar DHCP (utilice DHCP Options solamente si es necesario). Sin embargo, si así lo prefiere, puede en su lugar usar el método **Static IP address** para asignar direcciones WAN IP, Máscara de subred y Puerta de enlace predeterminada/Default Gateway) de forma manual.


WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.
Obtain an IP address automatically
Option 60 Vendor ID:
Option 61 IAID: (8 hexadecimal digits)
Option 61 DUID: (hexadecimal digit)
Option 125: Disable Enable
Use the following Static IP address:
WAN IP Address:
WAN Subnet Mask:
WAN gateway IP Address:

Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.

PASO 3: Esta pantalla proporciona acceso a la configuración de NAT, Firewall e IGMP Multicast. Active cada uno de ellos marcando la casilla adecuada ☑. Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.

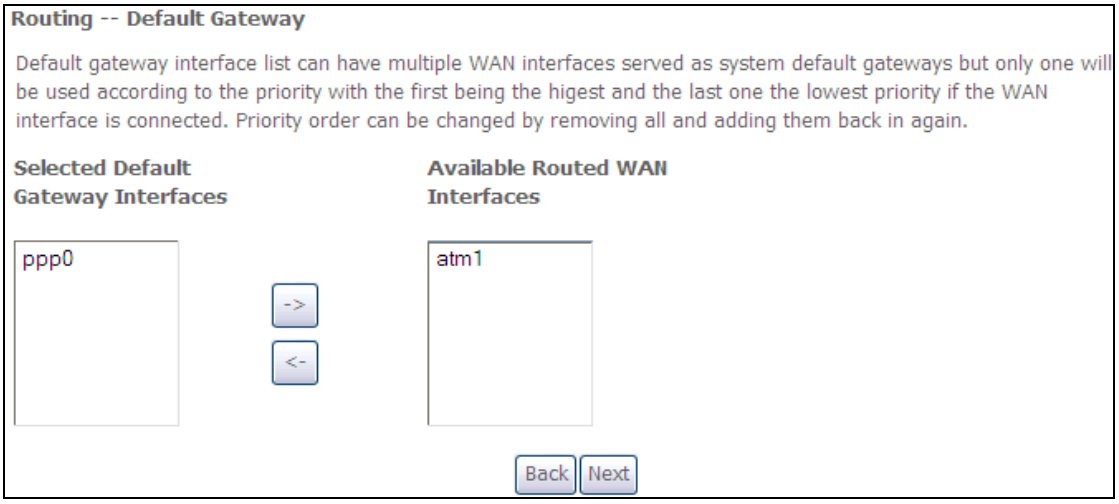

Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Enable NAT
Enable Firewall
IGMP Multicast
Enable IGMP Multicast
Back
Next

ENABLE NAT
Si la LAN está configurada con una dirección IP privada, el usuario debería marcar esta casilla ☑. El submenú NAT aparecerá en el menú Advanced Setup tras reiniciar. Por otro lado, si no se utiliza una dirección IP privada (p. ej. La LAN utiliza una IP pública), esta casilla ☑ no debería seleccionarse para liberar recursos del sistema y lograr un mejor rendimiento.

ENABLE FIREWALL
Si esta casilla ☑ está seleccionada se mostrará el submenú Security en el menú Advanced Setup tras el reinicio. Si el firewall no es necesario, esta casilla ☑ no se debería seleccionar para liberar recursos del sistema y lograr un mejor rendimiento.

ENABLE IGMP MULTICAST
Marque la casilla ☑ para activar Group Membership Protocol (IGMP) multidifusión. Este protocolo es utilizado por los host IPv4 para informar a cualquier router multidifusión cercano de los grupos multidifusión que tiene abonados.

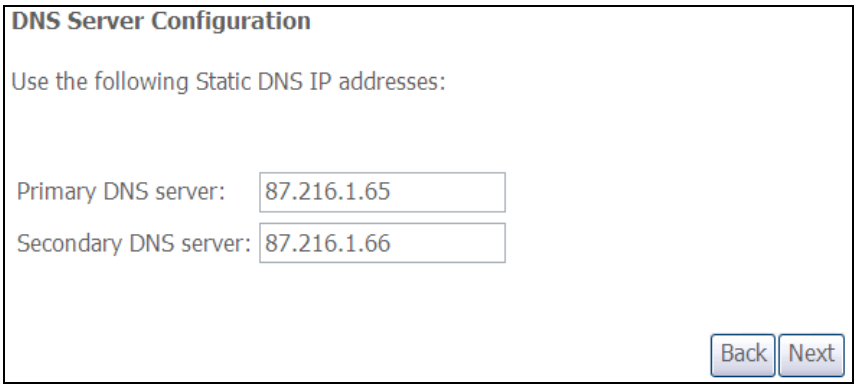
PASO 4:
Para elegir la interfaz que desea como pasarela predeterminada.


Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
ppp0
->
<-
atm1
Back
Next

Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.

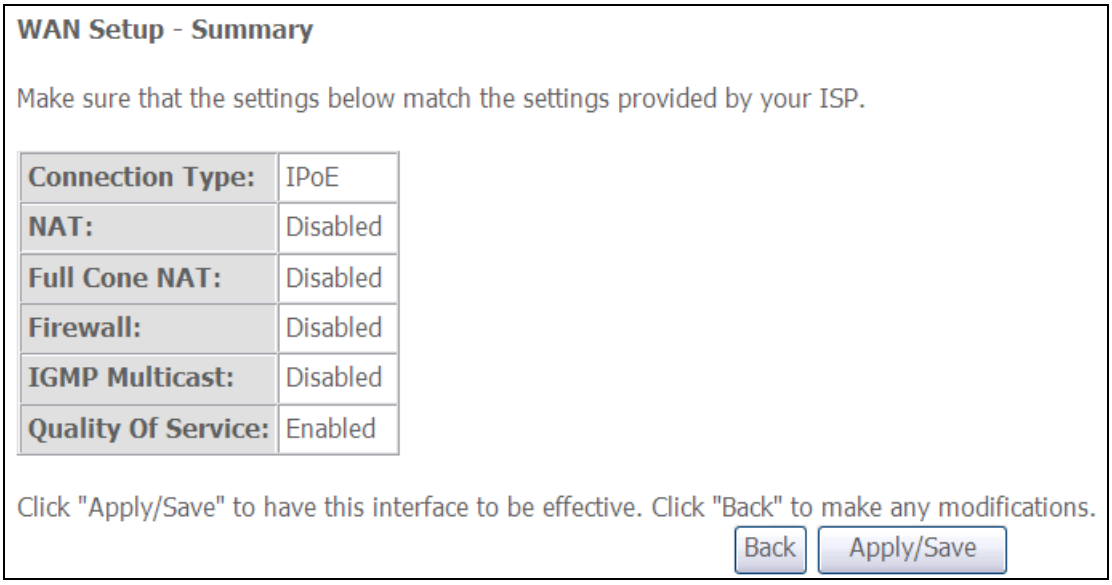
PASO 5:

Para establecer una dirección IP que el CPE usará para trasmitir la query DNS.



Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.

PASO 6: La pantalla WAN Setup - Summary muestra una vista general del servicio WAN que usted ha configurado. Compruebe los ajustes y haga clic sobre **Apply / Save** si son correctos, o haga clic en **Back** para modificarlos.

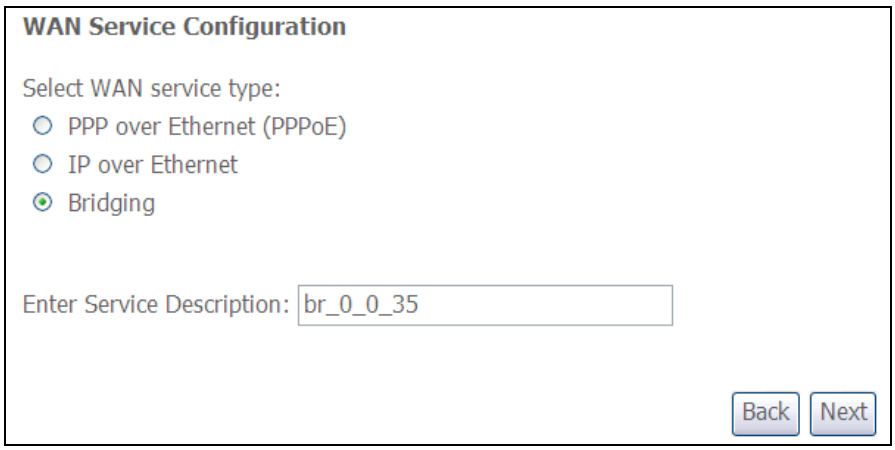

WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: IPoE
NAT: Disabled
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

Tras hacer clic sobre **Apply / Save**, el nuevo servicio aparecerá en la pantalla principal.
Para activarlo debe reiniciar el equipo. Diríjase a Management → Reboot y haga clic en **Reboot.**

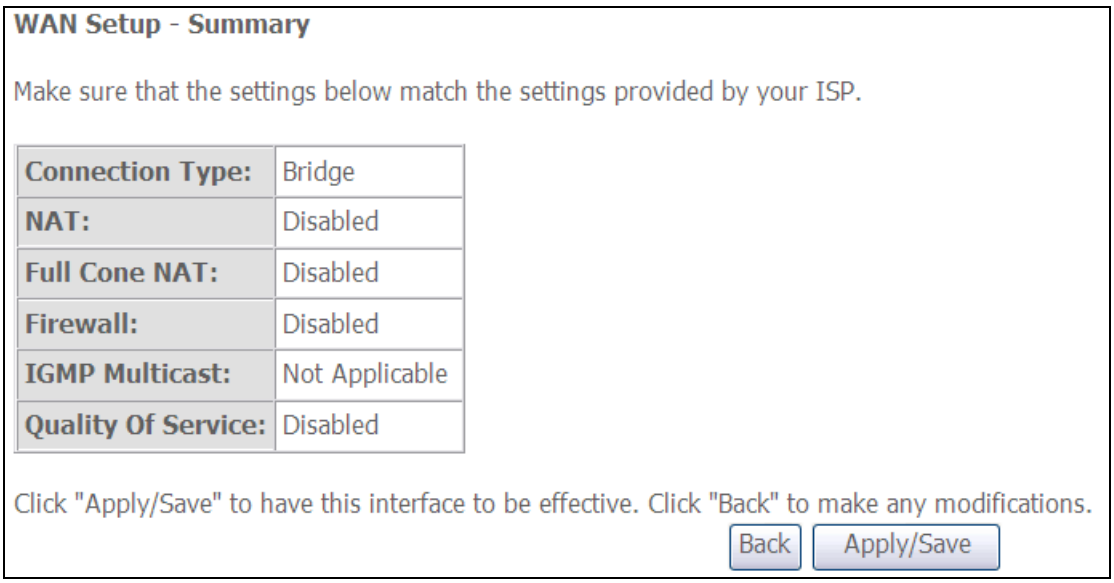
G2.3 Bridging (Puenteado)

NOTA:	Este tipo de conexión no está disponible en la interfaz WAN Ethernet.

PASO 1: Seleccione el botón de activación Bridging y haga clic en **Next**. También puede activar IPv6 marcando la casilla ☑ en la parte inferior de la pantalla.



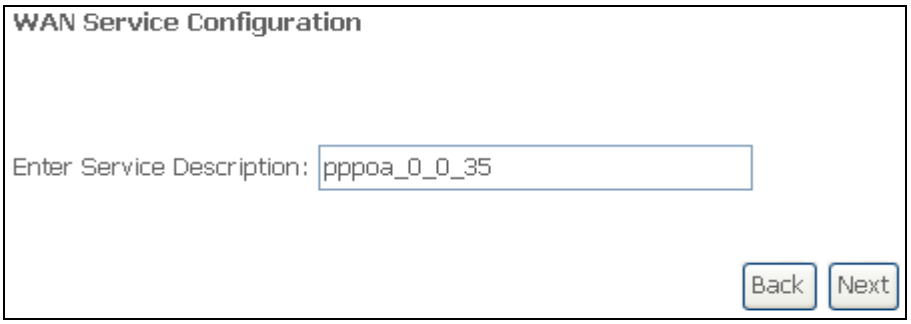
PASO 2: La pantalla WAN Setup - Summary muestra una vista general del servicio WAN que usted ha configurado. Compruebe los ajustes y haga clic sobre **Apply / Save** si son correctos, o haga clic en **Back** para volver a la pantalla anterior.


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: Bridge
NAT: Disabled
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Not Applicable
Quality Of Service: Disabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

Tras hacer clic sobre **Apply / Save**, el nuevo servicio aparecerá en la pantalla principal.
Para activarlo debe reiniciar el equipo. Diríjase a Management → Reboot y haga clic en **Reboot.**

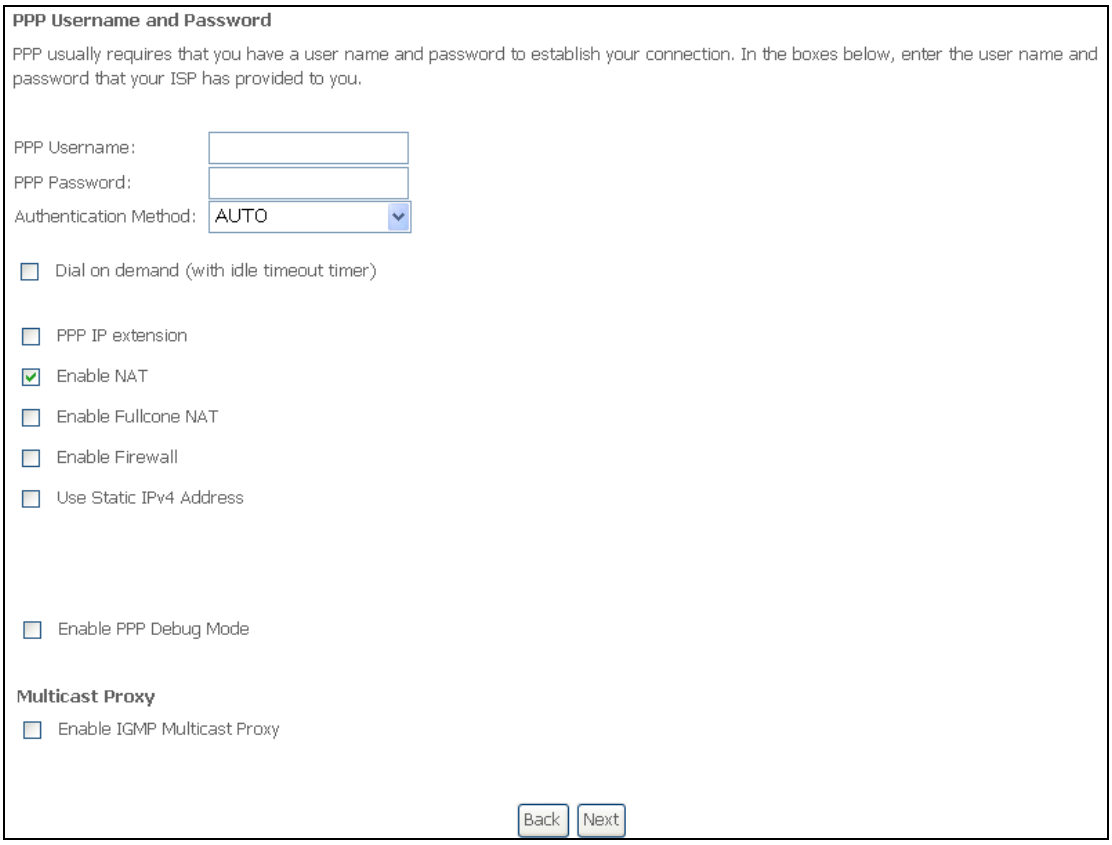
NOTA:	Si esta conexión de tipo bridge es el único servicio WAN, el AR-5387un no estará accesible para su gestión remota o soporte técnico desde la WAN.

G2.4 PPP over ATM (PPPoA)



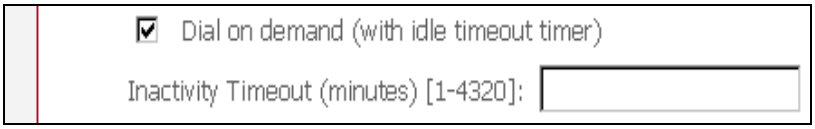
PASO 1: Haga clic sobre **Next** para continuar.

PASO 2: En la siguiente pantalla, introduzca la configuración PPP proporcionada por su ISP (proveedor de servicios).
Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.


PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
PPP Password:
Authentication Method: AUTO
Dial on demand (with idle timeout timer)
PPP IP extension
Enable NAT
Enable Fullcone NAT
Enable Firewall
Use Static IPv4 Address
Enable PPP Debug Mode
Multicast Proxy
Enable IGMP Multicast Proxy
Back
Next

PPP SETTINGS
El nombre de usuario y contraseña dependen de los requerimientos del ISP. El nombre de usuario puede tener un máximo de 256 caracteres y la contraseña un máximo de 32 caracteres de longitud. (Método de Autentificación: AUTO, PAP, CHAP, o MSCHAP.)

DIAL ON DEMAND
El AR-5387un se puede configurar de manera que se desconecte si no existe actividad durante un periodo de tiempo determinado marcando la casilla Dial on Demand ☑. También se debe introducir un periodo de tiempo de inactividad dentro del intervalo de 1 a 4320 minutos.



PPP IP EXTENSION
La extensión PPP IP es una función especial implementada por algunos proveedores de servicios. A menos que su proveedor de servicio requiera específicamente esta configuración, no la seleccione.

La extensión PPP IP hace lo siguiente:

- Solamente permite un PC en la LAN.
- Desactiva NAT y Firewall.
- El dispositivo se convierte en la pasarela predeterminada y en el servidor DNS del PC a través de DHCP y mediante el uso de la dirección IP de la interfaz LAN.
- El dispositivo extiende la subred IP en proveedor de servicios remoto al PC de la LAN. Es decir, el PC se convierte en un host perteneciente a la misma subred IP.
- El dispositivo puentea los paquetes IP entre la WAN y los puertos LAN a no ser que el paquete sea dirigido a la dirección IP de los dispositivos LAN.
- La dirección IP pública asignada desde el lado remoto usando el protocolo PPP/IPCP no se utiliza de momento en la interfaz WAN PPP. En su lugar, es reenviada a la interfaz del PC de la LAN a través de DHCP. Solamente un PC de la LAN puede conectarse de forma remota, ya que el servidor DHCP dentro del dispositivo solamente posee una dirección IP para asignar a un dispositivo de LAN.

ENABLE NAT
Si la LAN está configurada con una dirección IP privada, el usuario debería marcar esta casilla ☑. El submenú NAT aparecerá en el menú Advanced Setup tras reiniciar. Por otro lado, si no se utiliza una dirección IP privada (p. ej. La LAN utiliza una IP pública), esta casilla ☑ no debería seleccionarse para liberar recursos del sistema y lograr un mejor rendimiento.

ENABLE FULLCONE NAT
Esta opción se muestra accesible cuando está activado NAT. Conocida como NAT uno-a-uno, todas las peticiones desde la misma dirección IP y puerto interno son mapeadas a la misma dirección IP y puerto externo. Un host externo puede enviar un paquete a un host interno, enviando el paquete a la dirección externa mapeada.

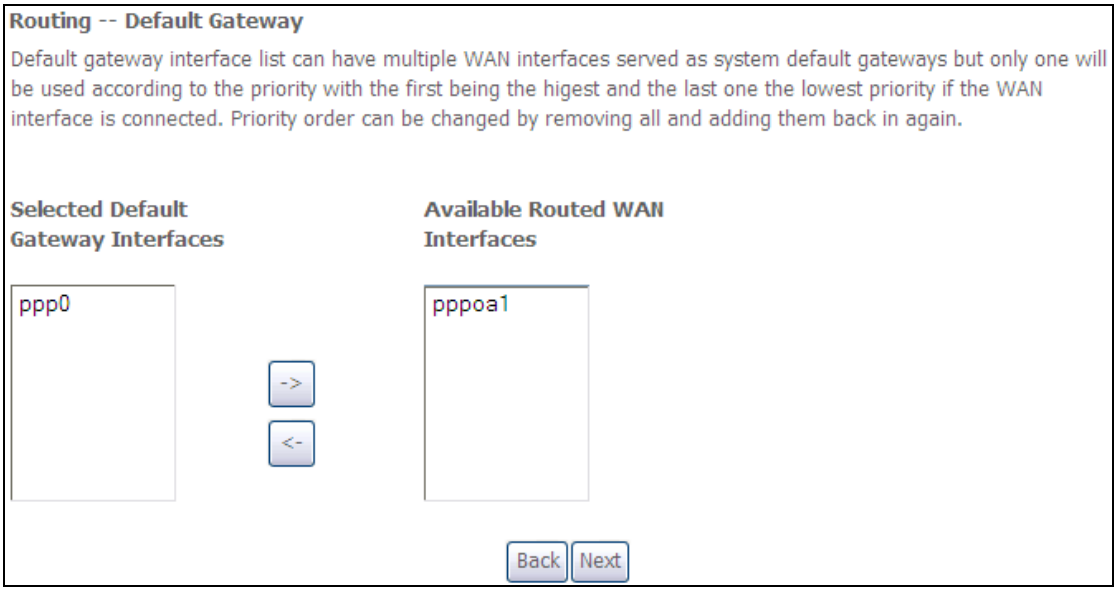
ENABLE FIREWALL
Si esta casilla ☑ está seleccionada se mostrará el submenú Security en el menú Advanced Setup tras el reinicio. Si el firewall no es necesario, esta casilla ☑ no debería seleccionarse para liberar recursos del sistema y lograr un mejor rendimiento.

USE STATIC IPv4 ADDRESS
A menos que su proveedor de servicios lo requiera expresamente, no selecione la casilla ☑. En caso de que debe seleccionarla, introduzca la dirección de IP estática en el campo IPv4 Address. No olvide ajustar la configuración de la IP en Static IP Mode como se describe en 3.2 Configuración IP.

ENABLE PPP DEBUG MODE
Cuando esta opción es seleccionada el sistema incluirá más información sobre la conexión PPP en el sistema de registro. Esto es lo indicado para la depuración de errores y no para un uso normal.

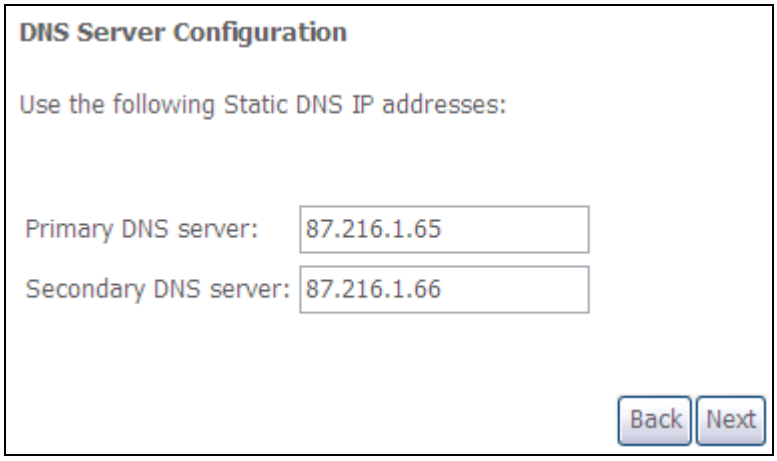
ENABLE IGMP MULTICAST PROXY
Marque la casilla ☑ para activar Group Membership Protocol (IGMP) multidifusión. Este protocolo es utilizado por los host IPv4 para informar a cualquier router multidifusión cercano de los grupos multidifusión que tiene abonados.

PASO 3: Seleccione una interfaz WAN como pasarela preferida por defecto.


Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
ppp0
pppoa1
->
<-
Back
Next

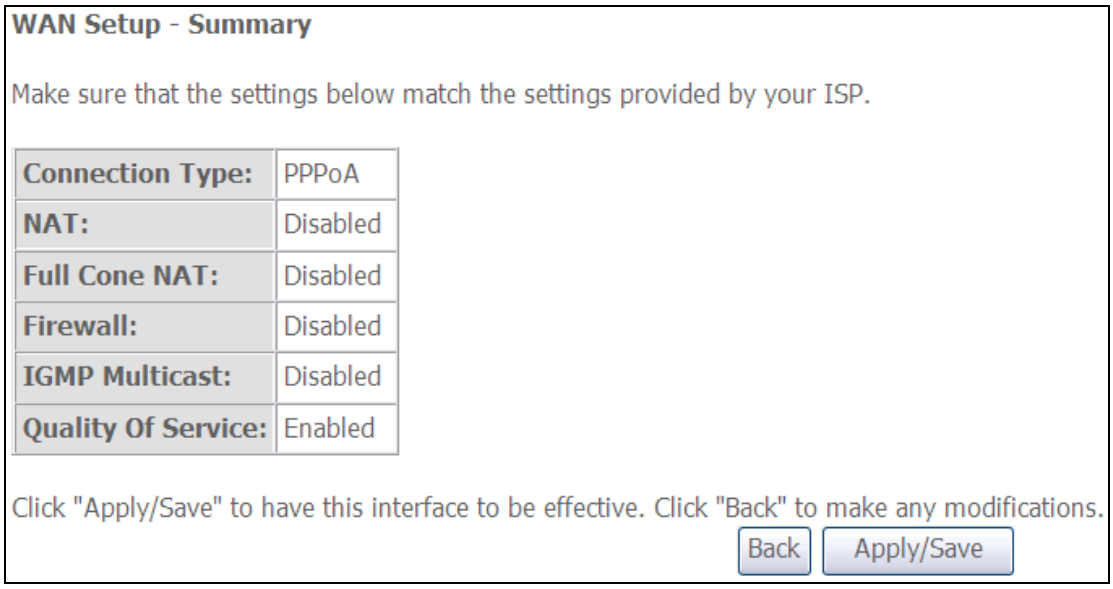
Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.

PASO 4: Seleccione una interfaz WAN o introduzca una dirección IP estática para el servidor DNS.



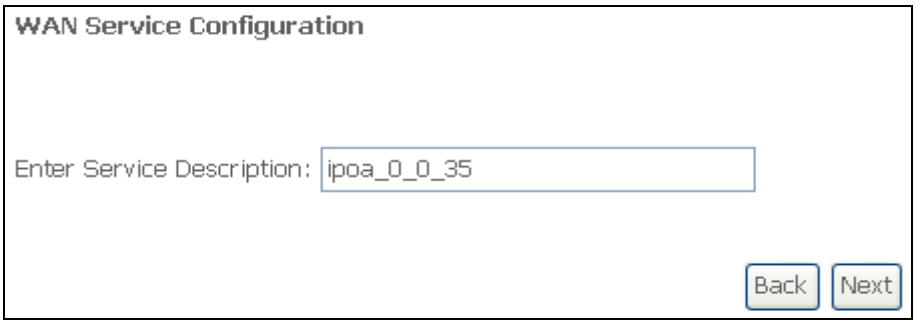
Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.

PASO 5: La pantalla WAN Setup - Summary muestra una vista general del servicio WAN que usted ha configurado. Compruebe los ajustes y haga clic sobre **Apply / Save** si son correctos, o haga clic en **Back** para modificarlos.


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: PPPoA
NAT: Disabled
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

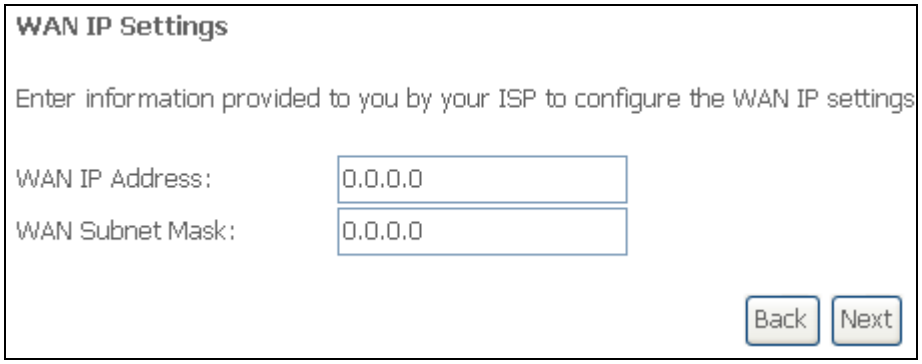
Tras hacer clic sobre **Apply / Save**, el nuevo servicio aparecerá en la pantalla principal.
Para activarlo debe reiniciar el equipo. Diríjase a Management → Reboot y haga clic en **Reboot.**

G2.5 IP over ATM (IPoA)

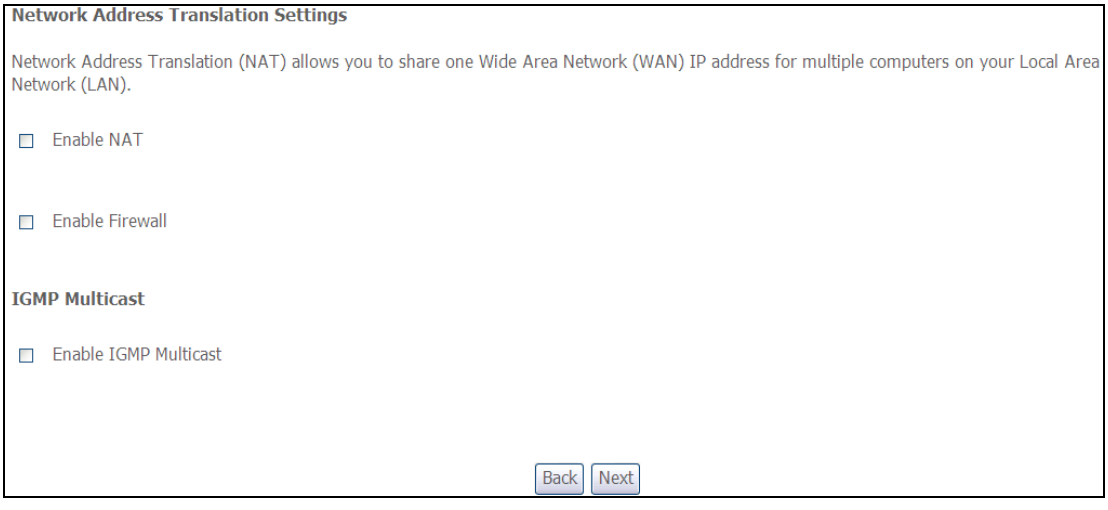


PASO 1: Haga clic sobre **Next** para continuar.

PASO 2: Introduzca la configuración IP WAN proporcionada por su ISP. Haga clic sobre **Next** para continuar.



PASO 3: Esta pantalla proporciona acceso a la configuración de NAT, Firewall e IGMP Multicast. Active cada uno de ellos marcando la casilla adecuada ☑. Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.


Network Address Translation Settings
Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).
Enable NAT
Enable Firewall
IGMP Multicast
Enable IGMP Multicast
Back
Next

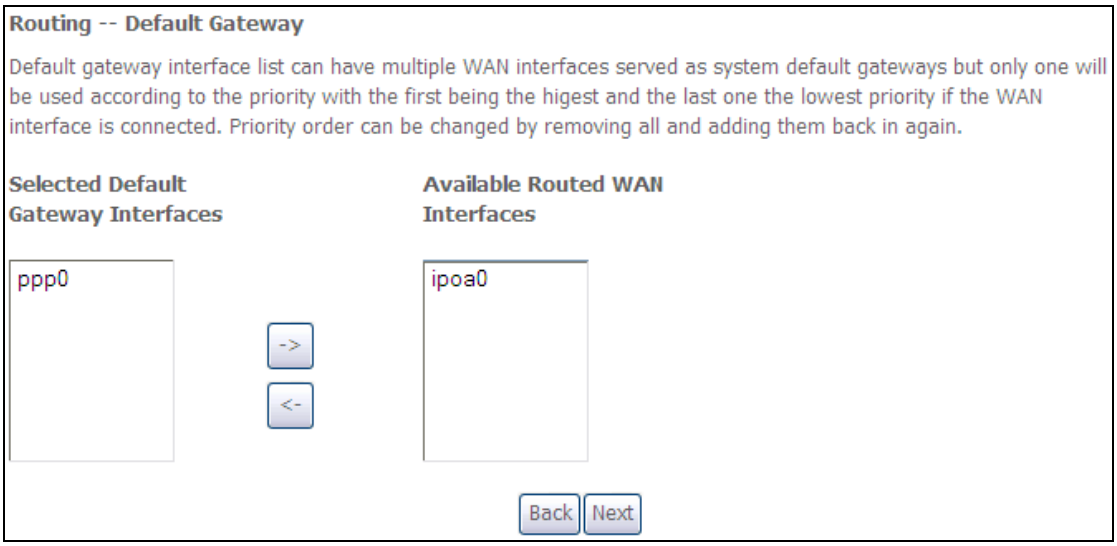
ENABLE NAT
Si la LAN está configurada con una dirección IP privada, el usuario debería marcar esta casilla ☑. El submenú NAT aparecerá en el menú Advanced Setup tras reiniciar. Por otro lado, si no se utiliza una dirección IP privada (p. ej. la LAN utiliza una IP pública), esta casilla ☑ no debería seleccionarse para liberar recursos del sistema y lograr un mejor rendimiento.

ENABLE FULLCONE NAT
Esta opción se muestra accesible cuando está activado NAT. Conocida como NAT uno-a-uno, todas las peticiones desde la misma dirección IP y puerto interno son mapeadas a la misma dirección IP y puerto externo. Un host externo puede enviar un paquete a un host interno, enviando el paquete a la dirección externa mapeada.

ENABLE FIREWALL
Si esta casilla ☑ está seleccionada se mostrará el submenú Security del menú Advanced Setup tras el reinicio. Si no es necesario el firewall, esta casilla ☑ no debería seleccionarse para liberar recursos del sistema y lograr un mejor rendimiento.

ENABLE IGMP MULTICAST
Marque la casilla ☑ para activar Group Membership Protocol (IGMP) multidifusión. Este protocolo es utilizado por los host IPv4 para informar a cualquier router multidifusión cercano de los grupos multidifusión que tiene abonados.

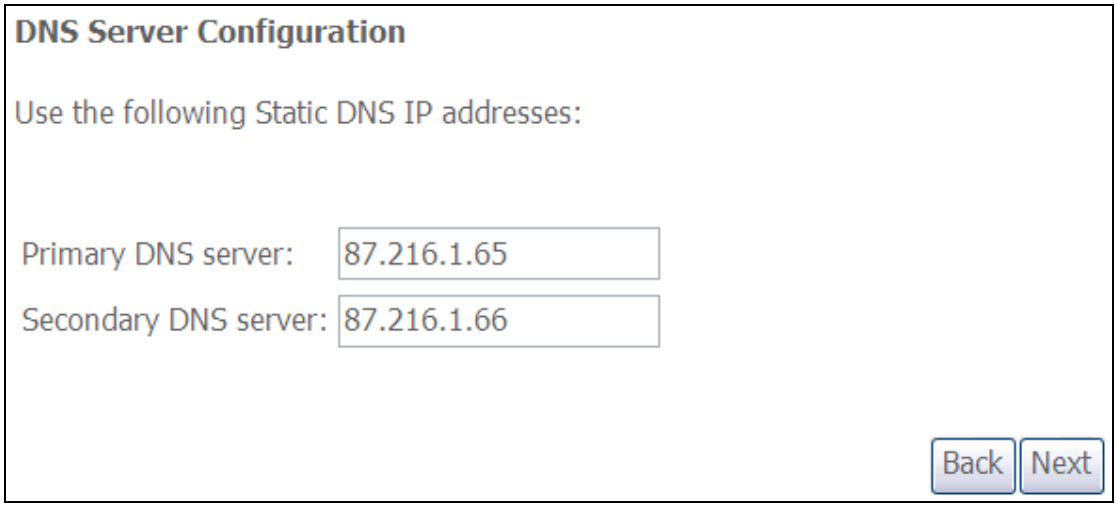
PASO 4: Seleccione una interfaz WAN como pasarela preferida por defecto.


Routing -- Default Gateway
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
Selected Default Gateway Interfaces
Available Routed WAN Interfaces
ppp0
ipoa0
->
<-
Back
Next

Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.

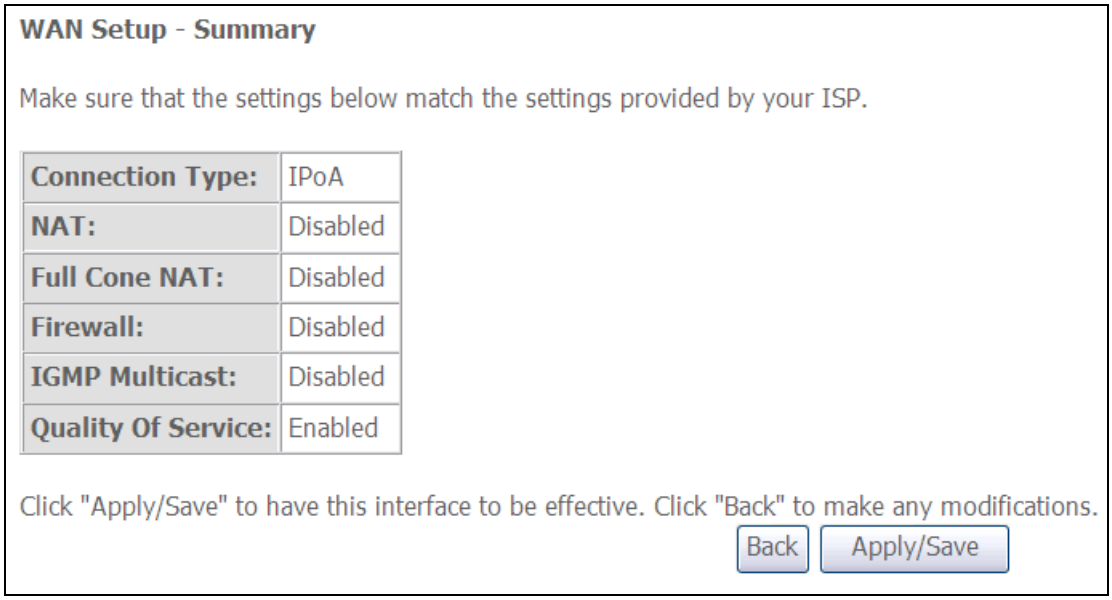
NOTA: Si el servidor DHCP no está activo en otra interfaz WAN entonces se mostrará la siguiente notificación antes de la próxima pantalla.

PASO 5: Selecciones una interfaz WAN o introduzca una dirección IP estática al servidor DNS.



Haga clic en **Next** para continuar o en **Back** para volver al paso anterior.

PASO 6: La pantalla WAN Setup - Summary muestra una vista general del servicio WAN que usted ha configurado. Compruebe los ajustes y haga clic sobre **Apply / Save** si son correctos, o haga clic en **Back** para modificarlos.


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: IPoA
NAT: Disabled
Full Cone NAT: Disabled
Firewall: Disabled
IGMP Multicast: Disabled
Quality Of Service: Enabled
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.
Back
Apply/Save

Tras hacer clic sobre **Apply / Save**, el nuevo servicio aparecerá en la pantalla principal.
Para activarlo debe reiniciar el equipo. Diríjase a Management → Reboot y haga clic en **Reboot.**